NTNU
Norwegian University of
Science and Technology

Security Requirements of Location –Aware Mobile Services

Department of Telematics, Autumn 2003 Tina Hermandsen Krekke

Preface

This project has been carried out within an in-depth project study course, "TTM4705 Information Security, Specialization" at the Norwegian University of Science and Technology. The author is currently completing her final year of the five years Master of Science Program within the field of Telematics.

Thanks to my project supervisor Stig Frode Mjølsnes for his input.

Trondheim, November 2003

_____
Tina Hermanden Krekke

Summary

As location-aware services are expected to be the "killer" application of future mobile and wireless networks, efforts are made on ensuring that a user's privacy will not be compromised. The aim of this project has been to enumerate and analyze multiparty security requirements of location-aware mobile services. The approach taken to analyse location-aware services in terms of security has been by looking at location models and threat models of location-aware systems in general. However, a particular effort by the IETF has been evaluated.

Location awareness rises from the fields of location sensing, mobile computing and wireless networks. This project identifies and discusses trends and challenges within these fields. Then possible location-aware services are briefly described, in terms of information services, tracking services, resource management, navigation and other services. As the fundamental for providing location-aware services are location information, different ways of representing location information are described next. Threats towards location aware systems and general security requirements are stated and an overview of some related work provided.

Then the Geopriv protocol, suggested by the IETF Geopriv (Geographic location/privacy) workgroup is discussed. Potential threats toward the protocol and its security properties are evaluated. The mission of the Geopriv WG is to create a privacy protecting protocol to be used when location information is transmitted, and assess authorization, integrity and privacy requirements that must be met in order to transfer geographical information. The WG is defining a Location Object which will allow a rule controlled disclosure of location information for location services. The information in the LO is secured according the rules set by the user.

The project is rounded off by summarizing security requirements discovered by studying other efforts, such as the Geopriv, and by common-sense reasoning. Generally, security requirements include:

- **Confidentiality** is required to prevent unauthorised disclosure of location information. Generally, users state rules regarding use, disclosure and retention of their location information, which location recipients must comply to. Such policies relate to **authorisation**.
- **Integrity** is required to prevent unauthorised modification of location information, and is typically accomplished by encrypting or digitally signing the information.
- **Availability** is required so that authorised entities are able to access location-aware services upon demand.
- **Accountability** is important as users should be held responsible for their actions. To accomplish this, user identification, authentification and authorisation is necessary. With respect to location information, users should be given the choice of identity (e.g. pseudonym, anonymity) and authentication is important to prevent impersonisation.
- **Non-repudiation** is to protect attempt by the sender to falsely deny sending the location information, or attempts by the recipient to falsely receiving the location information. This may be particularly important in legal cases.

These requirements are also discussed relating to emergency incidents, and the question of whether or not location awareness may be a tool for criminal activities are rised and answered. It do seem as the Geopriv protocol is a good choice when deploying location aware systems and services. The Geopriv Requirements [14] should at at least provide a guideline for security issues relating to location awareness.

Table of Content

Figures and Tables

List of Figures

List of Tables

Definitions, Abbreviations and conventions

This section provides some definitions, abbreviations and conventions used throughout this report.

Abbreviations

3G	3rd generation wireless networks
3GPP	3rd generation mobile system
A–GPS	Assisted Global Positioning System
AP	Access Provider
API	Application Programming Interface
BSC	Base Station Controller
BTS	Base Transceiver Station
CI	Cell identification
DoD	U.S. Department of Defence
DoS	Denial of Service
E – OTD	Enhanced Observed Time Difference
EOTD	Enhanced Observed Time Difference
EU	European Union
FCC	Federal Communications Commission
Geopriv	Geographic Location/Privacy
GMLC	Gateway Mobile Location Centre
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HLR	Home Location Register
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IrDA	Infrared Data Association
ISDN	Integrated Service Digital Network
ISP	Internet Service Provider
LAN	local area network
LBS	Location Based Services
LG	Location Generator
LIF	Location Information Forum
LMU	Location Measurement Unit
LO	Location Object
LR	Location Recipient
LS	Location Server
LTP	Location Technology Provider
MAC	Message Authentication Code
MD	Mediation Device
MLC	Mobile Location Center
MLP	Mobile Location Protocol
MNP	Mobile Number Portability
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station International ISDN number
NO	Network Operator
NR	Norsk Regnesentral (Norwegian Computing Center)
OECD	Organisation for Economic Co-operation and Development
OTDOA –IPDL	Observed Time Difference of Arrival – Idle Period Down Link
P3P	Platform for Privacy Preferences
PDA	Personal Digital Assistant

REG	Regulators
RH	Rule Holder
RM	Rule Maker
RX	Received Signal Strength
SIM	Subscriber Identity Module
SMLC	Serving Mobile Location Centre
SP	Service Provider
TA	Timing Advance
TLRS	Triggered Location Reporting Service
TOA	Time of Arrival
UL	Uplink
UMTS	Universal Mobile Telecommunication System
URI	Unified Resource Identifier
VLR	Visitor Location Register
W3C	World Wide Web Consortium
WG	workgroup

Conventions

In the following, location aware services, location aware applications and location based services will be given an equal meaning. Theoretically, location aware services will be services that are not dependent upon location to be present, whereas location based services are. Also, capital letters are used to identify Geopriv entities, e.g. Location Generator is an entity that generates the location information in a Geopriv context.

Definitions

Location Based Service	*a service that uses the location of the target for adding value to the service. Here, a location based service will also be referred to as a location aware service*
Target	*the entity being located.*

Chapter 1 Introduction

1.1 Background and motivation

At present there is a rapid development in the areas of mobile computing, wireless networking and location–sensing. This enables location–aware mobile services to be developed. Location-aware services are expected to be the "killer" application of the future mobile and wireless networks, as they add great value to the service in terms of personalisation. In general, a location-aware mobile service provides services to mobile users based on the location of a target. An example of a location-aware service is a "Buddy Finder" which enables the user to request the location of its friends.

In our increasingly mobile society, location will be critical for emergency services and mobile businesses in general. Clearly, location awareness adds value to both users and service provides and offer great potential for convenience. However, location–aware services also raise legitimate concerns about both personal and organisation privacy, as well as concerns about integrity and authenticity in emergency incidents. In addition, location awareness may provide new tools for criminal activity. It is utterly important that location-aware services are perceived as secure, in order for users to embrace them. This report focuses on determining a set of multiparty requirements for location–aware mobile services.

1.2 Problem Description and Scope

This project will aim to enumerate and analyze multiparty security requirements of location-aware services, and construct useful location- and threat models of such systems. A particular protocol to protect the privacy of the users of such location–aware mobile services, the Geopriv protocol (IETF), will be studied in depth to see how it will solve the security issues and threats that arise by using these applications. Supportive to this analysis, the project will identify and briefly describe the characteristics of interesting technologies for location-awareness.

This project will look at general security requirements of location–aware systems, and not delve into the technical security requirements of the underlying technology. The approach taken to analyse the security requirements of location–aware services has been by looking at a general location model of location aware systems, and by analysing potential threats towards such location–aware systems. A concrete scenario has been the Geopriv protocol. Hence, this project do not go trough all possible location –aware services that are available now, and that are likely to be available in the future. The project rather tries to capture some common–sense, general security requirements of location–aware systems. Also, current technologies able to provide us with location information will be described briefly. These technologies include satellite positioning systems, such as GPS/GALILEO and mobile terrestrial network, such as GSM and UMTS. However, security issues of these technologies will not be discussed, as I consider such issues to be without scope of this project. A brief discussion of security requirements that need to be present in emergency situations, as well as a brief analysis of whether location-aware services provides threats toward the society in terms of criminal activities or not, will be included.

1.3 Research Methods

This project has taken its form by looking at current research activities on this topic. The study has then been carried out as a literature study, limited to the area outlined above. It should, however, be noted that the location aware area is wide. The author has found other interesting efforts during this project which has been suppressed for further work.

1.4 Outline of this report

This project report aims at giving the reader an introduction to the technologies underlying location–aware service and provide an understanding of the security issues that raises from providing such services, e.g. in terms of privacy. Chapter 2 provides the reader with an introduction to interesting trends and technologies essential for providing such services, and conclude by looking at some of the security issues that such services bring forth. Chapter 2 also provides an overview of related work. Further on, Chapter 3 describes and comments on a particular suggestion by the Internet Engineering Task Force (IETF) called the Geopriv protocol. The Geopriv protocol aims at providing secure location information transfer and services in terms of privacy for all entities involved. Chapter 4 discusses security requirements of location-aware mobile services in terms of confidentiality, integrity, authorisation, accountability and non-repudiation. Finally, Chapter 5 concludes the project report, and aims at providing the reader with the conclusions that were made during the project.

Chapter 2 Location – Aware Mobile Services

The evolution of mobile computing, location sensing technology and wireless networking has created a new class of computing named *location - aware computing*[1]. A location–aware systems responds to a user's location, either spontaneously or when activated by a user request. Such systems might also utilize location information without the user being aware of it, i.e. by taking advantage of a nearby compute server to carry out some task.

In the USA, the Federal Communications Commission (FCC) has been acting as a driving force towards positioning standardization with their E911 services [1]. Outside the USA the development of such systems are mainly driven by commercial forces, as location –aware services may yield differentiation to services, reduce costs to network operators and increase the service provider's revenue. However, EU [2] has also adapted a recommendation that will help emergency services locate people. Also, Finland is currently considering a law that would allow parents to track their children via wireless phones. The proposed law could be a benchmark for privacy and wireless device use in the European Union.

This chapter will try to describe briefly some interesting technologies for location –awareness and the challenges we are facing by deploying such systems. Then possible location–aware services are outlined, before different ways of representing location information are looked into. Some security issues faced by deploying such systems will be identified towards the end of this chapter, and describe more thoroughly in both Chapter 3 and Chapter 4. Finally, the chapter will be rounded of by looking at current work on this area.

2.1 Trends, Technology and Challenges

Location– aware computing is made possible by combining three technologies; location sensing, wireless communication and mobile computing systems. In this section the current state of research in these three areas, and some future challenges are addressed.

2.1.1 Mobile Computing Systems

Hardware for mobile systems has made impressive progress over the past years. Mobile computing is commonly associated with small devices such as PDAs, mobile phones and laptops with wireless connectivity, which provides access to information processing and communication capabilities. These devices are now extensively used by the general public, and, though less visible, wearable computers [25] are beginning to make its entry in to specialised applications. But there exists a few issues, intrinsic to mobility, that complicate the design of such mobile systems [3]. These are listed and described below:

- Mobile devices are resource–poor relative to static devices.
- Mobility is inherently vulnerable. A laptop or a handheld machine carried by a mobile user is more vulnerable to theft than a desktop in a locked office. They are also more prone to accidental loss or physical damage. This, in turn, is a threat toward the privacy and confidentiality of the data that may be stored or accessed through these devices.

[1] Location –aware computing can bee seen as a part of context –aware computing. Context –aware computing refers to systems that recognize and react to real –world context. Context information include a number of factors, such as time of the day, the user identity, current physical location, weather conditions and possibly many more. The most critical factors of context are location and identity; hence, location –aware computing.

- Wireless connectivity is highly variable in performance and reliability. Some buildings (or areas, like a campus), offer reliable, high–bandwidth wireless connectivity, whereas others may support lower levels of bandwidth. This situation may be problematic in outdoor locations, where a mobile client may have to rely on a low–bandwidth wireless network with significant gaps in coverage.
- Mobile elements rely on a limited energy source. Battery technology seems to be improving slowly, and wireless transmission consumes a large amount of battery power.

Location–sensing technology can help mobile systems with these intrinsic issues. Location awareness may be used to guide a mobile user from a low–bandwidth area to a high–bandwidth area [4]. This technique, "cyber foraging", temporarily extends the resources of the mobile computer by pointing to remote resources that are found opportunistically. For example scenarios see [4]. Another suggestion includes the use of "infostations" to provide high –bandwidth connections for mobile devices. However, many problems must be addressed before the use of surrogates (infostations or the compute- and data–staging servers used in cyber foraging) can be accomplished transparently. Issues that must be considered include:

- Mechanisms to discover and select surrogates and negotiate their use.
- The computational, bandwidth, and power requirements of applications must be characterized in platform–independent ways.
- Techniques must exist to ensure and verify an adequate level of trust in a surrogate.
- The shared use of surrogates leads to questions of load balancing and scalability.

As battery stamina is a critical resource in mobile computing, new techniques and technologies should consider and adapt to battery state. A user may also pass, and use, multiple surrogates, so, how the surrogates fetch and cache data is an issue to be considered. These issues will, however, not be discussed any further, as it is consider out of the scope for this project.

2.1.2 Wireless Communication

There has been a growth in the deployment of wireless communication technologies during the past decade. The IEEE 802.11 family of wireless LAN technologies are now widely adapted, and Bluetooth is also implemented by many vendors. Infrared wireless communication (Infrared Data Association, IrDA) also plays a vital role, and is based upon the same technology that is used in TV remote controls.

It is difficult to foresee what new wireless technologies will emerge in the future, as well as which technology will be the most popular one. However, what is clear is that cheap, high-bandwidth, low power and ubiquitous wireless coverage will not be attained easily; hence, location–aware system will have to be designed to cope with this fact [5].

2.1.3 Location Sensing

This section gives a brief introduction to a few location–sensing systems used today. For a more thorough introduction, see [6,7]. The most widely known location-sensing system today is probably the Global Positioning System (GPS). It is commonly used for navigation purposes. A GPS unit receives signals from four or more satellites, with each signal carrying a timestamp and a description of the position of the satellite. By comparing this information, the GPS unit can calculate its own position. But, GPS do have some drawbacks:

- It does not work indoors.
- GPS satellite signals may be weak; hence, they do not always provide adequate coverage to all environments.
- Resolution of a few meters may not be adequate for all applications.
- Some applications may require coordinates relative to specific objects, but GPS uses an absolute coordinate system.
- The special components needed for GPS impose weight, cost and energy consumption requirements that are problematic for mobile hardware.

The satellite infrastructure is maintained by the U.S. Department of Defence (DoD) and it is not optimized for civilian use. A number of other mechanisms for location–sensing have been developed, and are being developed. For a summary of a few location–sensing technologies, see Appendix 1[5]. The EU plans to launch Galileo [8], a purely civilian equivalent to the U.S. GPS satellite network by 2008. It will also be more advanced, more efficient and more reliable than the current US GPS system, as it tries to address the shortcomings in the GPS system. It is expected to work with two different levels of services; a basic level, which is free of charge, and a restricted access service level for commercial and professional applications. Compared to the infrastructure of the GPS (24 satellites), Galileo will have 30 satellites divided between three circular orbits at an altitude of 24 000 km to cover the entire Earth's surface. They will be supported by a worldwide network of ground stations.

The mobile terrestrial network can also be used to determine the position of a mobile device, and is convenient as users of GSM networks keep increasing. Typical positioning methods in GSM include the method of cell identification (CI). As the CI method is not particular accurate, especially in rural areas, other methods should be deployed. For a brief introduction to location determination methods in GSM and UMTS, see Appendix 2.

No single location–sensing technology is likely to become dominant in the future. As Appendix 1 shows, there are a lot of dimensions along which location–sensing mechanisms can vary, and they need to be evaluated according to the degree of accuracy and precision, indoor versus outdoor use, battery consumption, and whether there is a potential loss of privacy for the users of the technology or not. Hence, the location–sensing technology is likely to depend on the usage context, and that, in the future, various technologies are likely to coexist. This is, however, not an advantage for location–aware software. It implies a need for technology–specific code, and makes it difficult to develop applications that can be used in a variety of location–sensing contexts. This is likely to slow the adoption of this new technology. Clearly, there is a need for a high–level, technology–independent application programming interface (API) for location sensing [5]. By using a technology–independent API application programmers do not have to consider the specifics of location sensing technologies. Creation of long-lived applications is supported too. The Location Information Forum (LIF) has proposed one such protocol, namely the Mobile Location Protocol (MLP). For more details see [9]. Basically, this protocol allows an application to query location information from a wireless networks, irrespective of underlying technologies and positioning methods.

Also, the fact that most location–sensing technologies are expensive to deploy today, will be a obstacle for the growth of location–aware computing. With GPS, for example, the end–user cost is relatively low, but the cost of the satellite infrastructure is enormous.

Given that it is possible to exploit location in a user context, what kind of services are we likely to see in the future?

2.2 Location –Aware Services

There is a wide range of different location–aware services, or location based services (LBSs), that may be offered in the future. Fundamental to these services are the fact that they are based on the location of the client. They offer the possibility to find/locate other persons, vehicles as well as tracking themselves. Clearly, a LBS consist of [10]:

- Obtaining the location of the user
- Utilizing this information to provide a service.

The request for location can originate from the client himself, or another entity. However, when a location is requested, the entity being located should give permission. LBSs can also be automatically triggered when the user is in a specific geographic location, i.e. location based billing.

There are three basic types of LBSs as identified by the GSM Association [10]: push, pull and tracking. In the case of a pull service, the user initiates a request for LBS. With the push service the request for service is made by the Service Provider, but the user must have given the Service Provider permission to send information to his mobile phone. Finally, tracking services are the 3rd basic type of LBS, and enable the user to track person by using a service provided by a Service Provider. A typical tracking service is the "Buddy Finder".

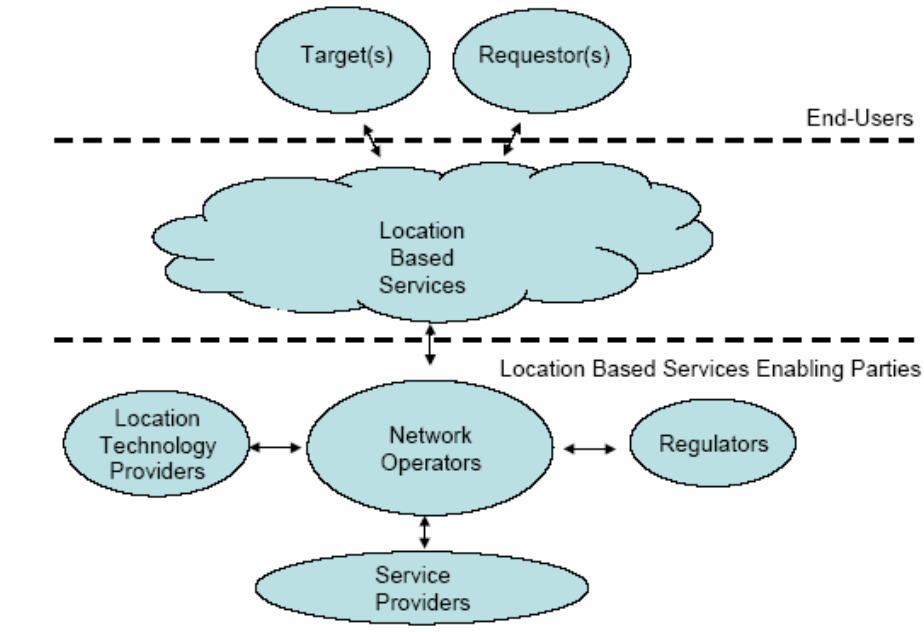


Figure 2-1: Players in LBSs [10].

Figure 2-1 shows the different parties that are likely to be involved in the provision of LBSs. As shown, the End–users can be the mobile user being located ("Target") or the user requesting some location ("Requestor"). Note that an End –user can take on both roles. The Location Based Services Enabling Parties is the Location Technology Providers (LTP), the Network Operators

(NO), Regulators (REG) and Service Providers (SP). The LTP are the manufacturers of different hardware and software which enables positioning of mobile terminals, where as the NO are the companies that have the infrastructure for GSM telecommunications. Regulators set up laws and regulations that guide how LBS can be implemented legally, with the major issue being privacy. Finally, the SP creates and provides LBS, which are accessible via NO.

Ericsson, being a LTP, has also provided a categorization of LBS, based on the type of applications they provide. The types of services include information services, tracing services, resource management, navigation and a general category named other services. Some service examples are provided below.

2.2.1 Information services

Information services make use of an information bank where information is filtered according to the relative position of a user and the applications he or she has selected. Examples of information services include location–based yellow pages, information about events and attractions ("What is happening today in Trondheim?").

2.2.2 Tracking services

Services can use location–based information to trace mobile terminals to provide safety, to prevent thefts, to improve delivery services and possibly many more. For example, to trace a stolen car, help locate persons quickly in an emergency situation, evacuation warnings and giving road side assistance personnel the location of a motorist in trouble. Emergency services will be discussed later in this report.

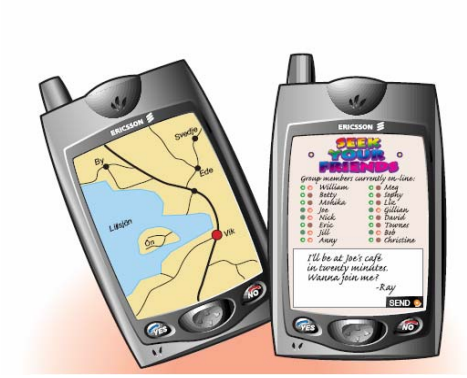


Figure 2-2: Example of a possible LBS ("Seek your friends") [11].

2.2.3 Resource management

Such applications are used to manage vehicle fleets, freight and service staff. Examples include taxi fleet management and administration of container goods.

2.2.4 Navigation

Navigation applications are used to inform customers about the best possible route from point A to point B. This can be used both for vehicle and pedestrian navigation.

2.2.5 Other services

Other services may include network planning, map services and location–based charging. From a network point of view, most wireless service providers already use location based services for internal operations, such as network planning, handovers, QoS improvements and traffic measures.

For LBSs to be widely accepted and reach the mass market, they require interoperability between operators, at a national and international level, and agreement with regard to international roaming and charging capabilities. Most importantly, issues such as privacy, and who owns the data and handles permissions must also be addressed.

2.3 Representing Location

Fundamental to location-aware systems are location information. This section aims at providing the reader with some possible ways of representing location information. Generally, location information can be represented in three ways:

- By physical location – grid based.
- By geographical location – hierarchical.
- By semantic location [33] – web like.

Physical location is represented by coordinates in a global coordinate system, and may be represented by latitude, longitude and altitude. Clearly, location information represented as physical location is not easy for users to comprehend, or express. Geographical location is a hierarchical way of representing location. For example, as Figure 2-3 shows, San Jose is represented as a city in California, in the United States. This way of representing location is easier for users both to express and comprehend, but as this is a hierarchical representation it may not be easy to add new locations and extend it. As these two ways of representing information carry little context information, researches at the CoolTown project at HP labs suggest using semantic location information. This is similar to a web like way of representing location, in which place is represented by a URI (Uniform Resource Identifier) [12], where links to a place may have other attributes such as physical/geographical location. Semantic locations are then globally uniform and unambiguous.

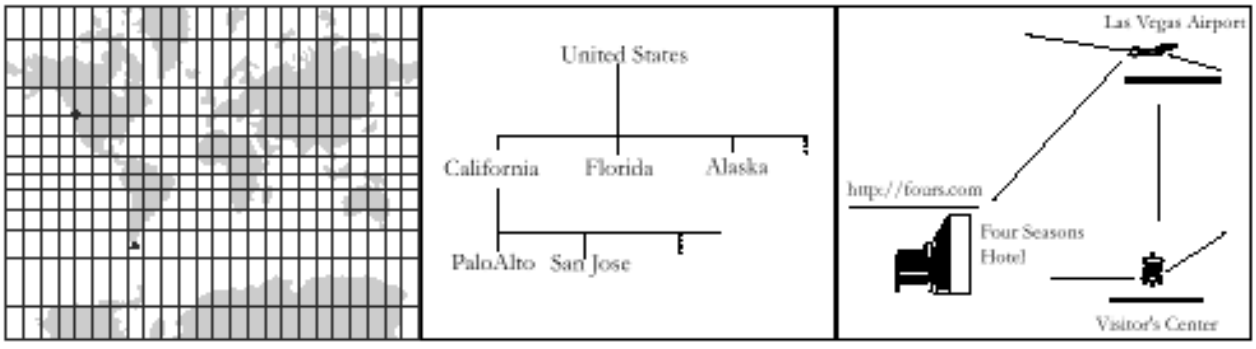


Figure 2-3: Physical, geographical and semantic location [33].

Associated with location information is typically the targets identity and time of which the location information was generated. Other attributes that could be associated with the location information is the speed and direction the target is heading in, as well as an indication of

accuracy. Lowering the accuracy of the location information generally provides a way of lowering the risk of invasion of privacy.

Typically, the location information will be presented in a 3-tuple like (id, location, time). The identity of the target could be the real identity, or some kind of pseudonym. In mobile communication, the targets identity is typically the MSISDN number. The location information can take on any of the forms discussed above, and time represents the time the location information where generated on. The time information may be coarsened as well. As time can be represented by a 3-tuple (hours:minutes:seconds), this gives an opportunity to represent time with different accuracy.

Location–aware application will have to accommodate geographical, physical and semantic ways of representing location information. Different location–aware applications may also need different ways of representing location. Clearly, it is not very convenient to have a friend's location represented by a physical coordinates upon request.

Different ways of representing the location information give different threats to privacy is. The following section proceeds by looking at general security issues in location –aware systems.

2.4 Security Issues

The increase in location–based applications makes protecting personal location information a major challenge. Clearly, location based applications offer great potential for convenience and productivity, but they do also introduce privacy risks for users that must be considered.

As the ability to pinpoint individual's location and the portability of mobile devices increases we could be facing systems were everyday activities and movements of individuals are tracked and recorded. This could in turn lead to a "Big Brother" society. As services that use location information may soon pervade our lives, it is important to consider the potential security issues such system raises, and in particular the privacy of the users. In the worst case, location information obtained could be misused by stalkers. Also, in order for a location–aware system to be embraced by the users, they need to feel that their privacy is not compromised. Hence, to maximize the success of such services and protect the users, privacy must be a core component.

Location information reveals the whereabouts of a user. This is a potential intrusion of privacy. A user may want to be notified about a location request, but it is also important to minimize the technology's intrusiveness and its demands of users. The user must have the ability to control the collection of location information. Consider a scenario where an advertiser can send advertisements to users currently in the area, notifying them about bargains. This will be beneficial to both the user and the advertiser, but its desirability and acceptability depends on the user's control over the advertising to which they are exposed.

Another issue important to consider is who controls the raw location data, and who computes the location. The raw position data can be obtained both from the users device or the network, where as the computation of the location information can be done by the users device, the network provider or possibly a third party. Clearly, there is a need for some rules to restrict access to such data, and that does not compromise the user's privacy.

The remainder of this section aims at describing threats towards location–aware systems, and general security requirements that should be present in such systems. A thorough discussion of security requirements will be given in Chapter 4.

2.4.1 Threat Model

A threat may be defined as a potential violation of security [15]. In a location–aware system context, location information and other data required to control the release of location information needs to be protected. Generally, threats include the following:

- Destruction of the location information and other sensitive data.
- Corruption or modification of the location information, or other sensitive data.
- Theft of a location–aware device.
- Interruption of service.
- Disclosure of the location information, or other sensitive data.

According to [15], threats can be classified as accidental or intentional and be active or passive. Accidental treats are those that exist with no intent, such as accidental release of location information to unauthorised parties. Intentional threats may in many cases be considered to be an "attack". Passive threat is such that if realized would not result in any modification to sensitive information in the system, where as active threats involve alteration of the information if realized. The remainder of this section briefly identifies a few specific types of attacks that may apply to location–aware systems.

Masquerade Attacks

A masquerade is where an entity pretends to be a different entity. For example, an authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges [15].

Replay Attacks

A replay occurs when a message, or parts of it, is repeated to produce an unauthorised effect.

Modifications Attacks

Modifications occur when some content, either in storage or in transmission is altered. This occur if, for example, "Allow Peter Peterson to view my accurate position at all times" is changed to "Allow Jon Jonsson to view my accurate position at all times", when Jon is not authorised.

DoS Attacks

Denials of Service (DoS) occur when an entity fails to perform its function and deliver its service.

Insider Attacks

Insider attacks occur when legitimate users of a system behave in an unauthorised or unintended way.

Outsider Attacks
Such attacks may use techniques such as wire tapping, intercepting, masquerading as authorized users or by bypassing authentication and access control mechanisms.

Clearly, a location–aware system should try to prevent all these threats. The next section presents an overview of security requirements that should be present in such systems. A more detailed discussion is provided in Chapter 4.

2.4.2 General security requirements

Generally, the following security requirements must be present in a location–aware mobile system:

- **Privacy** is the protection of personal information, or **Secrecy**, the protection of organisational information.
- **Confidentiality** is the prevention of unauthorised disclosure of location information.
- **Integrity** is the prevention of unauthorised modification of location information. Integrity includes the detection and correction of modification, insertion, deletion or replay of transmitted data.
- **Availability** is the prevention of unauthorised withholding of information or resources. The system must be accessible upon demand by an authorised entity.
- **Non–repudiation** is required to prevent either sender or receiver from denying a transmitted message.

The above stated security requirements are multiparty requirements, that is, all the parties involved in a location transaction will demand that these security features are present. In a location–aware computation, there will be a requestor, or recipient, requesting the location of a target, or a device. Trust relationship may not exist between all parties in such exchanges; hence, users must be able to express rules (policies) regarding use of their location information. Some of the current system suggestions are based upon the use of user rules or policies.

2.4.3 Related work

There is a lot of ongoing research on this area, as people acknowledge the need for security, and in particular privacy, in the emerging location–based services. The topic of privacy is extremely important, and should be reflected in systems handling personal information. A lot of nations, including Norway, have got their own privacy legislations to reflect this as well. In Europe, most of these are based upon the EU–directives [16], and in general they are based upon the OECD Guidelines for Fair Information Practices [17]. The remainder of this section briefly look at ongoing work in this area.

- **Geopriv**. The Internet Engineering Task Force (IETF) Work Group (WG) Geopriv (geographic location/privacy) is proposing a set of requirements in their Internet Draft [14]. The working group aims at assessing the authorization, integrity and privacy requirements that must be met in transferring location information. This protocol will be discussed and evaluated in Chapter 3.
- **LIF (Location Inter-operatbility Forum)**. LIF was established by Motorola, Ericsson and Nokia in 2000 with the aim of resolving interoperability issues related to the development and deployment of mobile location services solutions. LIF has stated a set of

guidelines for location data privacy. These guidelines are being used in LIF specification work, and are contributed to other standardisation bodies. The guidelines are based on the fair information principles of the OECD [17], regulatory requirements and expected demands from customers. These guidelines are intended to help anyone developing Mobile Location Services better comply with privacy. See [32]. LIF has also defined a Mobile Location Protocol (MLP) which enables location aware applications to access location information independent of the underlying technologies [9].

- **Norwegian Computing Center (Norsk Regnesentral)**. The Norwegian Computing Centre has identified a need to let the user's explicitly formulate their personal location privacy policy. For more information see [20], [21], [22] and [23].
- **P3P**. Also P3P [18], the Platform for Privacy Preferences Project, which was developed by the World Wide Web Consortium (W3C), is a simple, automated way for users to gain more control over the use of personal information on Web sites they visit.
- **pawS.** A privacy awareness system for ubiquitous computing environments [19], pawS, proposed by Marc Langheinrich. He argues that totally perfect protection for personal information will hardly be achievable, and propose to build a system that help others respect our personal privacy, enable us to be aware of our own privacy, and to rely on social and legal norms to protect us from the attackers of our privacy.

Through out the rest of the report the Geopriv protocol will be considered. This choice is made because they are specifically focusing on the privacy of the users. The Geopriv WG suggest a protocol that can be deployed on existing technologies, and with the primary goal of protecting the security and privacy of the users. The next chapter looks at the requirements towards privacy as stated by the WG, and possible threats toward it.

Chapter 3 The Geopriv Protocol

In this chapter the authorization, security and in particular privacy requirements of location – based services will be discussed and described, as proposed by the IETF Geopriv workgroup [14,34]. The Geopriv workgroup has identified a need to securely gather and transfer location information for location services, and at the same time protect the privacy of the users. First, this chapter introduces a location model for the Geopriv protocol. The protocol must be usable in situations with constrained devices with low bandwidth and/or computing power, which is the characteristics of mobile devices. Then, threats towards the Geopriv protocol will be analysed, and finally, security properties will be discussed.

3.1 Entities

A basic location model for the following discussion is shown in Figure 3-1 below. Note that the entities shown may not necessarily be separate physical entities.

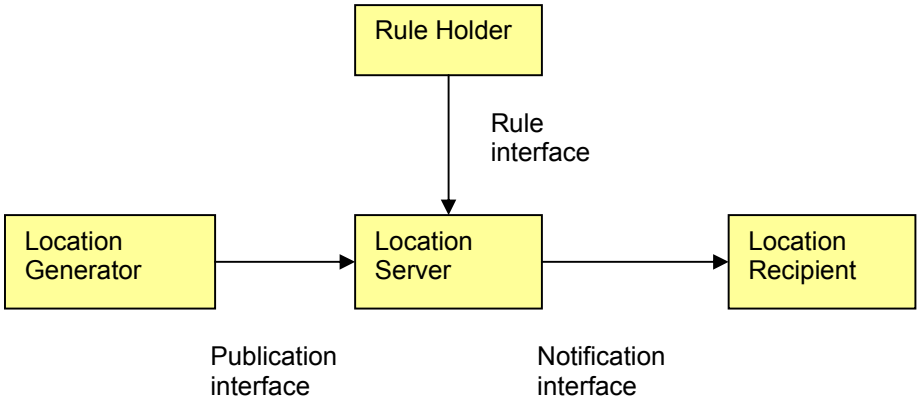


Figure 3-1: Location Model of the Geopriv protocol [14]. Note that the entities may not be separate physical entities, and that this model does not make any assumption about how location information is provided.

The Location Generator (LG) is the entity that initially determines or gathers the location of the Target. How this location information is obtained will not be discussed any further, please refer to section 2.1.3 for a brief introduction to different Location–Sensing technologies. The Target may be a device (i.e. a mobile phone being a proxy for the location of the Target), a person (i.e. the owner of the mobile phone), a ship or truck. In general, the target is an entity whose location is desired by a Location Recipient (LR). Also, the LR and the Target may be the same entity. Upon gathering the location information about a Target, the LG creates a Location Object (LO) describing this location. The LO is a technology–independent object conveying location information and possibly privacy rules to which security mechanisms can be applied. When the LG has created a LO, it publishes it to a Location Server (LS). The LS in turn receives queries from LRs, and applies rules/filters to the LO according to the rules defined by the Rule Maker (i.e. the owner of the Device). The Rules will be discussed more thoroughly in section 3.1.1. The location information (or the filtered location information) will then be sent to the LR, which may receive location information either by explicitly asking LS for it or by receiving it asynchronously. The following section describes the rules, or policies, in Geopriv.

3.1.1 Privacy Rules

The privacy rules regulate activities relating to a target's location and other information, such as the collection, use, disclosure and retention of location information. They specify how location information may be used by an entity, and must be obeyed. They may also define how the location information should be filtered, depending on who the recipient is. Filtering [14] is the process of reducing the precision or the resolution of the data. For example, a user may not want everyone to know what particular café he or she is currently visiting. Rather, the rules could state that the information provided should be something like "I am in Trondheim city", not the accurate location.

Generally, these rules should be based on fair information practices (such as the OECD Guidelines on the Protection of Privacy and Transporter Flows of Personal Data, see [17]), and are defined by a Rule Maker (RM). Usually, this will be the owner of the device being located, or it might be the user who is in possession of the device. Parents, for example, may want to control what happens to the location information derived from their children's mobile phones. A company may own a mobile phone and provide that one to an employee, and then let the employee set its own privacy rules. There are, however, four scenarios where constraints or overrides may be placed on the rules defined, as identified by the Geopriv WG. These are listed below:

- **Emergency services.** In the case of an emergency, laws may require that accurate location information should be transmitted.
- **Legal interception.** In the case of criminal actions, laws may require that accurate location information should be transmitted, or that logs of location information can be accessed.
- Owners of particular locations may impose **constraints** on the use of privacy rules.
- **Governmental authority** may impose constraints on the use of privacy rules in non – emergency situations as well.

Finally, the rules are stored in an entity called Rule Holder (RH). The RH provides the rules associated with a particular target for the distribution of location information [14]. It may push rules on to a location server, or a location server may pull rules from the RH. Rules should be stored in a standardized way, in order to provide for interoperability. Policy rules are discussed in [37].

Upon receiving a location request from a LR, the LS applies the rules according to the LR and sends the, possibly, filtered location information. Appendix 3 provides the interested reader with a few possible location scenarios in Geopriv.

3.2 Threat analysis

This part of the chapter aims at analyzing threats against the geopriv protocol architecture, in particular threats that result from the storage of data by entities in the architecture, and threats posed by the abuse of information yielded by geopriv. This discussion is based upon [24].

3.2.1 Motivation for the attackers

Clearly, the most obvious reason for attack towards the geopriv, and any location –aware systems, are to learn the location of a Target who wishes to keep its location private. It might also

be that an already authorized LR wishes to obtain location information with a greater degree of precision than the RM desires. There are, however, other potential motivations for an attacker. These include:

- Prevent a Target's location from being distributed.
- Modify or corrupt location information in order to misrepresent the location of the Target.
- Redirect the Target's location to a 3rd party that is not authorized to know this information.
- Identify associates of a Target.
- Learn the habit or routines of a Target.
- Learn the identities of all the parties that are in a certain location.
- Halt the operation of the entire geopriv system, i.e. though a Denial of Service attack.

Some attackers might also be authorized as legitimate participants in the geopriv protocol exchange and abuse this location information. This includes the distribution or accumulation of location information outside the parameters of agreements between the principals, possibly for commercial purposes or as an act of unlawful surveillance. The different motivations for attackers, give rise to different types of possible attacks toward the suggested geopriv protocol. Those will be discussed in the following section.

3.2.2 Attacks toward the Geopriv protocol

There exist various kinds of attacks. The following section looks at attacks towards the geopriv protocol, to the hosts and to the use of the protocol.

Protocol Attacks

In this section, the different types of possible attacks toward the Geopriv protocol will be analyzed. Possible protocol attacks include eavesdropping and/or interception, masquerading, identity spoofing, information gathering and Denial - of - Service attacks.

Eavesdropping and/or Interception

Consider a scenario where a LR has access to very coarse location information about a Target, but wishes to learn the accurate position. There is a number of ways in which that could be realized. First of all, the LR might eavesdrop on one of two network connections, either the connection between the LG and the LS or the connection between the LS and some LR that receives unfiltered and precise location information. The last part, however, requires the LR to know someone that obtains precise location information.

Masquerading

The LR may also try to access accurate position information by masquerading, that is:

- Impersonate a LR that has access to precise location information to the LS, in order to receive the unfiltered information.
- Impersonate the LS to the LG.
- Attempt to act as the RM, hence, provide rules to the LS that would enable the attackers' access to uncoarsened location information.

Identity Spoofing

It is clear that if the identity of entities able to view location information for a specific Target is compromised, the privacy is threatened. Anyone inside or outside the transaction that is capable of impersonating an authorized entity can gain access to confidential information – such as the identity and the location of a Target, or initiate false transmissions in the authorized entity's name. An attacker might also try to spoof network traffic from the LG to the LS or spoof traffic from the LS to the LR. The goal of the attacker is to provide false location information or possible replay a genuine LO, about a Target.

Information Gathering and Traffic Analysis Threats

The possibility to eavesdrop on a network connection and intercept traffic can create traffic analysis[2] threats as the interceptor collects more data over time. Traffic analysis threat creates the risk of eavesdroppers determining the Target's associates, and may allow an eavesdropper to ascertain the identity or characteristics of the target in a particular location and learn about its associates. The information carried within the LO is secured in a way compliant with the rules stated by the RM (user). Other information i.e. carried in other objects or headers are not secured in the same way. Hence, it may not secure the Target against general traffic analysis attacks. If the attacker is able to intercept the plaintext location information as well, and generate a log of this data, analysis could reveal regular routes and typical behaviour patterns.

Denial of Service (DoS)

If an attacker wanted to deprive entire networks of geopriv services, rather than attacking particular users, it is likely that the effort would be focused on the LS. The LS plays an important role in managing access to location information in many scenarios. It also looks as though the geopriv protocol have some opportunities for *amplification attacks*. When the LG publishes location information, the LS may act as an exploder - potentially delivering this information to numerous targets. If the LG provides very rapid updates of position, then it could be problematic provided that there is a large number of possible LR. Operations associated with the LS may require cryptographic authentication. This is imposing a computational expense on the LS. The fact that the LS will have to verify credentials presented by these geopriv messages provides attractive means for attackers to flood the LS with dummied geopriv information that is spoofed to come from a LG, LR or the RM. Hence, floods of geopriv information could have grater impact than DoS attacks based on generic packet flooding.

Countermeasures

To avoid protocol attacks, the following security properties and countermeasures should be present in geopriv:

- Confidentiality is required for both the connection between the LG and the LS and the connection between the LS and any given LR.

[2] Traffic analysis threats exist when the eavesdropper can determine by the very fact of the network transmission, that a relationship between the various entities involved exist. Traffic Analysis is an attack in which the adversary monitors certain parts of the system to be able to match a message sender with the recipient or, in particular for mobile systems, to locate or track movements or sender or receiver [35].

- A LS must be able to authenticate and authorize LRs, in order to prevent impersonation. The LS must also be able to authenticate RMs, to avoid situations where unauthorized parties can change rules.
- A LG must be able to authenticate and authorize LSs, in order to prevent impersonation.
- The LS need to authenticate the LG.
- The LRs must be able to authenticate LSs.
- The location information must be protected from replay attacks[3].
- The RM must be able to define Rules regarding the use of their Location Information.
- LSs must be capable of authenticating LRs to prevent impersonation, as well as authentication RMs to ensure that unauthorized entities cannot change rules.
- The LS must use stateless authentication challenges and similar measures to ensure that authentication attempts will not unnecessarily consume system resources.
- The RM must be able to publish policies in which the rate at which the Location Information is sent is limited in order to prevent amplification attacks.

Host Attacks

This section looks at threats towards data stored at servers and in the devices as well as information that are contained in rules. For example, the location information maintained at a server is subject to many potential risks.

- By negligence, carelessness or lack of knowledge, the server may **accidentally** release the location information to the wrong LR, or simply just fail to properly filter the information that he sends to the various LRs.
- On the other side, the server may **intentionally** be misusing the location information, i.e. by selling a Targets or a LRs "profile" despite what he or she might have stated in the Rules. It is also likely that users with authorised access to the server may decide to misuse the access to obtain location information about a Target.
- There is also the risk of someone **outside** the system hacking into server in order to retrieve location information.
- Last, there is a possibility that someone will use the **legal system** in order to obtain an individual's records from the server. In this case, the Target's location information is likely to be released without noticing the Target.

It is difficult to determine the possible threats of individual devices, as geopriv is required to work with any given technology or device. Any device that maintains information it requests and/or receives is exposed to the similar threats as a LS. There is a lot of ways that data may be compromised. For a device with a screen, there is always a possibility that another individual will have the opportunity to view the display without the user's knowledge. If the device provides verbal feedback (i.e. to give direction to the blind), there is an additional potential for the Location Information to be compromised. Also, if the Target is sitting in an public place requesting a map telling directions from the Target's home to another location, anyone who can see the device output might be able to learn where the Target live, its identity and possibly more. Location information is also compromised if the device, with a maintained log of location

[3]Replay Attack: An attack in which a service already authorized and completed is forged by another "duplicated request" in an attempt to repeat authorized commands. [30]

information, were lost or stolen. This would enable someone other than the RM to access information regarding who the location information was sent to and when, and possibly the location of the Target during the transaction. Access to this information will enable an entity to determine significant private information such as who the owner of the device has associated with in the past, the locations where the Target has been and for how long. That is, habits and routines could be abstracted.

The Rules a RM creates may also reveal information either about the RM or the Target. If an entity had access to a log of data at the LS or at a Device, knowledge of the Rules would enable decoding of the location information to something more accurate. Hence, protecting the rules is important too.

Usage Attacks

Weak or absent default privacy rules in the geopriv protocol may compromise the location information. With no default privacy rules, it is likely that a large number of devices would reveal the location information by default. Privacy rules should control the collection, use, disclosure, and retention of Location Information, and must comply with fair information practices, see [17].

Most individuals will lack the skill or motivation to create privacy rules to protect their location information. Then, with no privacy rules concerning this information, they will be vulnerable to various attacks. Consider a situation without default rules where the mobile device is signalling out to anyone nearby at regular intervals its whereabouts, responding to anyone who queried it with its full location information, lets the Location Servers pass its position on to anyone etc. Clearly, and according to the Geopriv working group, default rules are necessary to address this problem.

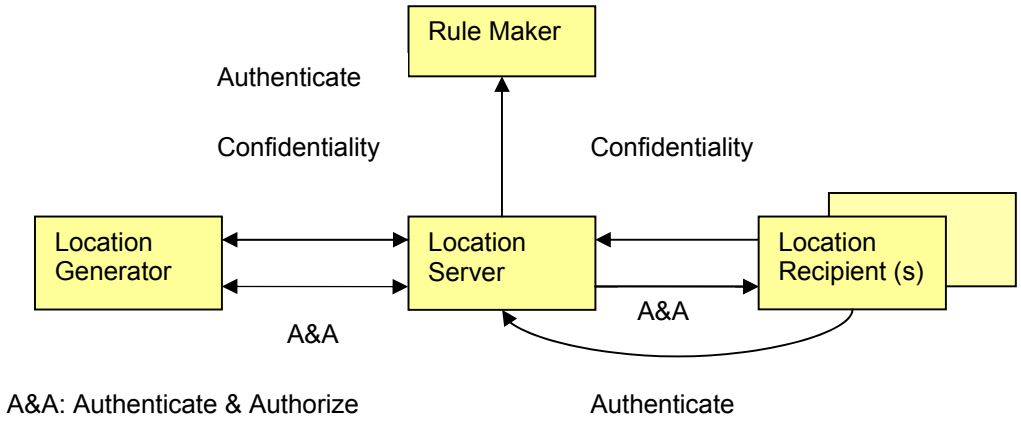


Figure 3-2 Security properties of Geopriv

Figure 3-2 shows a summary of the security properties outlined in this section. In the following sections general security properties of the protocol will be discussed.

3.3 Security Properties

With location–based services, the ability to gather and generate a target's location, and access derived location information, clearly raises privacy issues. When considering a target's privacy,

central elements are the identities of entities that have access to raw location data, derive or compute location, and /or have access to derived or computed location information. The key issue is whether or not these entities can be trusted to know and obey the privacy rules of the user.

There are three security properties of Geopriv important to note. Clearly, securing the Location Object itself is important to guarantee integrity and confidentiality of the location information. It will also be important to authenticate the sender and the receiver of the LO. Also, the privacy rules play an important role towards a user's privacy and security. Finally, the ability of a user to be identified by a different identity, e.g. a pseudonym, is important to be able to provide privacy. These three aspects will be discussed from a security point of view here.

3.3.1 Security during transmission

Security during transmission of data is, clearly, very important. The connections between the LG and the LS, the LS and the LR and the LS and the RM should be secure, so that the LO cannot be compromised during transmission. Encrypting the location information, that is, the LO, would enforce secure transmission. In addition:

- **Mutual end-point authentication** should be present. Authentication is crucial to the security of location information during transmission. The LS must be capable of authenticating LRs to prevent impersonating, and the LG must be capable of authenticating LSs to ensure that raw location information is not sent to improper entities. Additionally, LSs must be able to authenticate RMs to ensure that unauthorized entities cannot change Rules.
- **Data Object integrity and confidentiality.** The LO must maintain integrity at all points of communication between LSs and LRs. Confidentiality is required on both the connection between the LG and the LS, as well as the connection between the LS and any given LR. Confidentiality of Rules sent over the network to the LS is also of importance. Encryption and digital signatures would provide such security properties.
- **Replay protection.** Replay protection prevents an attacker from capturing a particular piece of location information and replaying it at a later time in order to convince LRs of an erroneous location for the target. Both LRs and LSs may need replay protection.

The full set of requirements as stated by the Geopriv WG is found in [14], section 7. Their document state requirements for the Location Object, requirements for the protocol carrying the LO, about the Rules, for identity protection, credential requirements, and security features of the LO. The following security features will be provided by the LO:

- **Mutual end–point authentication:** the protocol transferring the LO is able to authenticate both parties in a LO transmission.
- **Data object integrity:** the LO is secured from modification by unauthorized entities during transmission and during storage.
- **Data object confidentiality:** the LO is secured from eavesdropping during transmission and during storage.
- **Replay protection:** an old LO may not be replayed by an adversary or by the same entity that used the LO itself.

The LO will also implement a minimum of crypto algorithms, i.e. for digital signatures and encryption. It may also implement security mechanisms like message authentication codes

(MACs). Also, the protocol should allow bypass if authentication fails the case of an emergency. This is important, because we do not want emergency calls to fail due to a failed minimal authentication.

3.3.2 Rules

As mentioned, the privacy rules set by the user play an important role in securing the location information, and it is utterly important that it is being obeyed. The Geopriv WG suggests that:

- The RM should **define Rules**. The RM for a device, i.e. the user of, or owner of, the device, or both, should define rules regarding collection limitation and the use of the information.
- Geopriv should define **default rules**. The RM should be free to change his or her Rules to provide more or less protection. However, to protect privacy and physical safety, default Rules should, at a minimum, limit disclosure and retention of location information. Default Rules are also important to protect a LG, i.e. if an LG is unable to determine the Rules set by the RM before publishing the LO to a LS, it is important that some default Rules protect the LO in transit. And further, to ensure that the LO is only sent to authorised LRs. The RM should be able to determine the content of these default Rules at any time.
- **LRs should not be aware of all rules** defined by the RM. They only need to be aware of those Rules it must obey.
- Certain **rules should travel with the LO** [29]. The RM has no real control over what is done with the Location Information once it arrives at the LR. Hence, if certain rules travel with the LO, the RM can encourage the LR to obey the rules, i.e. rules can prevent the compilation of a log of a Target's location information on any device. Allowing rules to travel with the LO has the potential to limit the opportunity for traffic analysis attacks.
- Rules may **disallow a certain frequency of requests**. The RM might be able to set a Rule that disallows a certain number of requests made within a specific period of time. This could prevent attackers from detecting patterns in randomly coarsened data, and prevent LRs from sending repeated requests to gain more accurate presence information. Thresholds on notifications of location information can help to combat amplification attacks.

The rules itself may be accessible to a LS in a number of different ways and will be secured in different ways. The rules may be stored in a public or non-public Rule Holder (RH). Rules in a public RH will typically be digitally signed, where as rules in a non-public RH will be authenticated using a MAC or a signature. Rules may also be carried as a part of the LO, and be secured as a part of the LO. Finally, rules may be presented by the LR as capabilities or tokens. A token may be issued by a RM to a LR expressing an explicit consent of the RM to access the location information [14]. The token will typically be digitally signed.

3.3.3 Protection of identities

Protection of identities is an important countermeasure towards the threats to location information as well. The user should also be able to specify which identifier (i.e. local identity, pseudonym or private identifier) is to be bound to the location information, and should also be able to hide the real identities of himself and his partner to all entities of the protocol. Identities are an important component of the LO. Some form of identification of the Target, RM and LR will be necessary for authentication, but there are methods to separate these authentication

"credentials" from the true identity of the devices. This is useful in situations where the log of location information is compromised. By protecting the identities threats to privacy when the Target's identity is stripped is minimized. Geopriv suggests two ways of protecting the identities:

- **Short-lived identifiers** to protect the Target's identity.
- **Unlinked Pseudonyms**[4] to protect LRs' identity.

Short–lived identifiers allow the protocol to hide the true identity of the RM and the Target from the LS and LRs. The identifiers would still provide authentication. However, making the identifiers short-lived helps prevent any association of a true identity of a Target with particular habits and associates. Unlinked Pseudonyms may protect the identity of the LR in the same manner as short–lived identifiers are protecting the identity of the Target. Reasons for the target to hide its real identity should be clear. Reasons for hiding the real identity of the LR include: a) the information can be used to infer the real identity of the Target, b) knowledge of the identity of the LR may embarrass the Target or breach confidential information, and finally c) can give information on habits and movements.

When using both these techniques to hide away identities, any record that the Location Server had of the transaction would have two "credentials" associated with a location information transmission. One would be linked to the Target, the other one to the LR. These "credentials" would allow the LS to authenticate the transmission without ever acquiring knowledge of the true identities of the individuals associated with each side of the transmission. Protection of identities should be considered in scenarios involving an unintended target. See Appendix 3.

3.4 Security Issues in Emergency Scenarios

In the case of an emergency, it will usually be better to reveal the accurate position, then not. There are three different cases in which the authentication in an emergency call may fail:

- The emergency server may fail to authenticate itself.
- The user may not authenticate itself.
- The user and the emergency server do not authenticate themselves.

First, when the emergency server fail to authenticate itself, the user should be given the choice to write a rule specifying what should happen. For example, the user could specify a rule saying "send the location information anyway". Second, what should you do when the authentication fails because the user is not authenticated? Is it reasonable to apply a rule stating: send the location information to the emergency server. What about the third situation? Is it reasonable to send the location information anyway? There might be security threats that must be considered. Currently, Geopriv do not go into depth about these issues, but rather acknowledges that considerations must be taken and are working on an Internet draft specifying it. Chapter 4 will identify some requirements relating to emergency services.

[4] Unliked Pseudonyms: the protocol transferring the LO should be able to hid the real identity of the Rule Maker, the Target, and the Device, to LSs or LRs, if required by the Rule Maker [14]. The protocol should also be able to hide the real identity of the LR to the LS.

Chapter 4 Security Requirements

This chapter aims at summarizing some of the security requirements mentioned in the previous chapters. It also aims at giving the reader a set of concrete requirements that should be present in a location aware system. In this chapter, the requirements will be discussed according to the general security requirements described in section 2.4.2.

4.1 Confidentiality

Confidentiality can be defined as the prevention of unauthorised disclosure of information [28], and it is about not letting unauthorised users read, or learn, sensitive information. Sensitive information can be classified as information that is sensitive to an individual, or information that is sensitive to an organisation, and this relates to privacy – being the protection of personal data, and secrecy – being the protection of data belonging to an organisation [28].

Privacy is the protection of personal data. Both the users of systems involving personal data and possibly national governments, or both, may impose this requirement. As previously mentioned, privacy will be a key success factor for location–aware systems. In Chapter 3, the IETF Geopriv workgroup suggests letting the uses define rules, or policies, regarding the use, retention and disclosure of their personal location information. As mentioned in 2.4.3, other efforts also suggest using user controlled policies. Based on these observations, it seem as though a future method for letting user control the release of their location, should be based on user controlled policies. With regard to the location based advertisement briefly mentioned in section 2.4, the user should be able to specify rules regarding release, and use, of their information.

As concluded by the Geopriv WG, such systems should include default rules as not all users will be able to define their own rule sets. However, users should easily be able to override these default rules, and specify their own. Default rules are necessary because a lack of rules would probably allow release of location information to anyone interested, with no limitations regarding retention and use at all. This scenario must be avoided.

Also, parents should be allowed to specify rules for their children. Companies, who provide their employee with a mobile phone, should let the employee set his own privacy rules. The company may, however, specify rules regarding “on-work” information release in order to protect information belonging to the organisation (secrecy). The company may for example specify that the identities of communication parties should not be revealed during “on-work” time because the fact that those two parties are communicating, may reveal sensitive information.

The user may state rules disallowing a certain frequency of requests. This is to prevent attackers from detecting patterns in randomly coarsened data, and prevent location recipients from repeatedly sending requests to gain more accurate information. Rules may also depend on laws in the country the user resides in. This complicates things when the mobile users a moving between countries, and roaming on different networks. As a baseline, all actions should be checked against rules in the user’s home country, or network. However, the rules that apply for the country the user is currently visiting cannot be ignored.

Threats toward privacy may be detected using a “Privacy Violation Detection” tool, as proposed by [22]. A privacy violation detector monitors access to personal data and detects misuse and/or

anomaly behaviour. For ways of actually enforcing privacy policies [22] provides some useful points.

The user should also be told when they are being located. However, the intrusiveness of location-aware services should be minimized. Hence, users may decide to be told statically per service, or dynamically on a per service or per location request basis. The notifications may e.g. be provided to the user as a log. The user should also have the opportunity to enable/disable location services, and whether they want to be located or not.

The location information should also be marked, or time stamped, so that a receiver of location information cannot further distribute it without permission, at least not to unauthorised parties. The Geopriv suggests that some policies should be transmitted along with the LO, so that the receiver of the LO are explicitly told about the rule regarding that information.

Privacy, and secrecy, can also be accomplished by reducing the accuracy of the location information and by identifying the users by pseudonyms, or other "non–real" identities. This will typically also be stated in the user defined policies. By reducing the accuracy of the location information, some users will be able to pinpoint, whereas others are only told the name of the city. The user should also be given the possibility to be anonymous.

A location–aware system also needs to be protected against insider attacks, such that personnel operation a location server cannot redistribute, or sell location information about users. To avoid this, personnel must be selected carefully, mechanisms for auditing must be present so that such attacks can be detected, and system configurations must be carefully selected.

To avoid situations where outsiders are able to intercept the transmitted location information, and possibly read or learn it, confidentiality is required between all entities in a location–aware system. This can be accomplished by encrypting the location information, but traffic analysis threats may still be possible. The Geopriv WG suggests that the LO should support identity protection, and that the LO must support a minimum of cryptographic algorithms, for digital signing the LO and for encryption the location information. Encryption of the location information would yield confidentiality. Encryption may also reduce the likelihood of a successful replay attack, traffic analysis attacks and repudiation.

Finally, if a users' device is stolen or lost, this will compromise the confidentiality. This is in particular so if the device maintains a log of location information. If coupled with, say, the policies stated and real identities, privacy is compromised. Threats by people peaking over "my shoulder" can only be avoided by acting carefully with sensitive data. Logs also raise additional concerns. For how long should people be allowed to store my location information? Generally, logs should only be kept for a short time, and then discarded. This should typically be stated in rules. Also, to avoid storing location in mobile devices, handset-based location solutions should be avoided. That is, only handset-assisted solutions should be supported, as the location information would then be kept in the network. With a handset-based positioning solution, the position calculation is carried out in the mobile device, where as with a handset-assisted positioning solution, the device only makes measurements.

Generally, user's privacy settings are only allowed to be compromised in the case of an emergency incident or by lawful interception.

4.2 Integrity

Integrity may be defined as prevention of unauthorised modification of information, and includes the detection and correction of modification, insertion, deletion, or replay of transmitted data including both intentional manipulations and random transmission errors [28]. Integrity should be present in location–aware systems and services. It is important that a receiver of location information is confident that the location information it received is accurate, at least to the degree of precision agreed upon with the target.

Encryption is one way of providing integrity. Encryption also makes it harder to launch replay attacks, traffic analysis attacks and repudiation. Digital signatures can also provide for non–repudiation.

Integrity of the rules stated by the "owner" of the location information is important too. If the integrity of the rules is compromised, that is, an unauthorised entity is able to modify, insert or delete some of the rules, the privacy will be compromised. Due to this, rules may have to be digitally signed in order to prevent modifications.

Clearly, integrity is essential in emergency situations. A user of a location–aware emergency service wishes to be sure that its position is transmitted without modifications, in order to be sure that the help will get there. On the other side, emergency service "servers" also want to be sure that the emergency position that they received is not modified, or replayed. This will require some kind of encryption.

4.3 Availability

Availability may be defined as the prevention of unauthorised withholding of information or resources, and is the property of a system being accessible and useable upon demand by an authorised entity [15]. We want to ensure that a malicious attacker cannot prevent legitimate users from having reasonable access to theirs systems, that is, we want to prevent DoS [5] attacks and other flooding[6] attacks to the system. As identified in Chapter 3, the Geopriv system may have a potential for amplification attacks. This is particularly critical if the "Location Server" need to perform some cryptographic authentication check. Due to this, the Geopriv suggest that such a location server should be using stateless authentication challenges.

Availability of location-aware systems is in particular important when it comes to emergency services. When in an emergency, users want the emergency service to be available and accessible. Also, the end-user response time should be minimal on an emergency service.

4.4 Accountability

Accountability is also an important security requirement as users should be held responsible for their actions. To accomplish this, identification and authentication of users are necessarily. Users' actions must also be authorised.

[5] The prevention of authorised access to resources or the delaying of time –critical operations [28].
[6] E.g disabling a server by overwhelming it with connection requests.

4.4.1 User identification

As identified in Chapter 3, the user should be given the possibility to be anonymous, or choose other identities than its real identity. The ability to be anonymous is an important concept of privacy. The user should be given the possibility to take on either a pseudonym, a short–lived identifier, be anonymous or use its real identity. This may also be specified in policies. In GSM anonymity is preserved by an Opaque ID, see [10].

4.4.2 Authentication

The target must be able to authenticate the parties that receive their location information based on their identity, and vice versa. This is to prevent impersonation. As mentioned in section 0, authentication should be based on using stateless authentication challenges to avoid amplification attacks. A location server applying rules to location information prior to releasing it must also authenticate the rules, or the "rule–server". The placeholder for the rules must in turn authenticate the policy owner as well, so that no one can impersonate the policy owner to change to policy.

4.4.3 Authorisation

To avoid attacks that breach confidentiality, integrity and availability, authorisation is important. Authorisation is related to the existence of a security policy, which is a set of rules that specifies which actions are permitted and which actions are prohibited [28]. This relates to the fact that the target must be able to authorize release of their location information in a location –aware system. In such a system this should be provided by user defined policies. It is important to make sure that no unauthorised entity can alter the policy, that is, the "Rule Maker" must be authenticated.

As suggested by the Geopriv WG, recipients that are authorised to access location information may receive a token. Typically, such a token should be authenticated or signed.

4.5 Non – repudiation

Non–repudiation is about providing evidence so that the target cannot deny being at a location for where it released its position. This is in particular important for legal aspects. The recipient of the location information may want proof of the origin of data, and the sender of the data may want proof of delivery of the data. Such proofs will protect attempt by the sender to falsely deny sending the information, or attempts by the recipient to falsely receiving the information.

This requirement may be particularly important when considering emergency scenarios. An emergency server wants to make sure of the origin of the location information. A user of the emergency server may also want to be sure that the location information was in fact delivered to the server.

4.6 Other issues

This section aims at describing a few issues associated with location –aware systems not yet mentioned in great details. These issues, however, do not directly relate to security requirements of location-aware systems. These issues may be for future work.

4.6.1 Convenience

Clearly, it is important that location–aware systems, and applications, are easy to use in order for users and service providers to use such systems. The speed of location information retrieval is

also important. Hence, it is important not to overload such systems with cryptographic check, as that tends to slow down systems. Clearly, there is a trade off between convenience and security. As identified in this project, security is important, as users of such system must feel that their privacy is protected in order to uses it. Users also wish for services that are easy to administer, so that it is easy to enable/disable the service. Also, the interaction between the user and the service should take into account the users profile and terminal capabilities.

4.6.2 Standardization

The fact that such systems should be convenient to use, relate to the fact that they should be standardized. As users of mobile systems inherently are mobile, they will occasionally be roaming on other networks. However, services of their home network should still be accessible. To enable this, it is important that network operators agree upon some standard in order to enforce interoperability. For a discussion on roaming and interoperability in GSM see [10]. It is also important that the mobile devices and visited networks support the same positioning method in order for location services to work outside their home network. This will not be an issue for services that is based on CI methods. However, for services based on the accuracy provided by more advanced methods, such as E-OTD, OTDOA or A-GPS (see Appendix 2), this will be an issue. There also exist various ways of implementing the different advanced methods, such as the A-GPS, which could lead to difficulties when roaming. For example, an A-GPS handset-based device in a network that only supports handset-assisted modes, will not work.

4.6.3 Criminal activities

With the potential that lays within location-aware mobile services it may provide new tools for criminal activities. This fact has not been discussed in this project report, but it is clear that such system should allow legal systems to bypass rules set by users in case of illegal activities. That is, it should be possible to track people in the case of criminal activities.

It is clear that location-aware systems must be secure, and in particular, the user must be able to control the release and retention of its location information. This relates to privacy – the protection of personal information. Moreover, systems and services providing location-awareness should be available upon request of an authorised entity, and make sure that confidentiality, integrity and non-repudiation is ensured.

Chapter 5 Conclusion

The aim of this project was to determine a set of security requirements for location-aware mobile services. It is clear that security mechanisms must be present in location-aware systems. If location-aware services and location-aware systems fail to provide security mechanisms, location-awareness will not be embraced by the potential users. Security requirements such as confidentiality, integrity, availability, accountability and non-repudiation apply to location-awareness. These were discussed in Chapter 4, and are briefly recaptured here:

- **Confidentiality** is required to prevent unauthorised disclosure of location information, and prevent unauthorised users learning sensitive information. Users can help control their location information by defining policies relation to e.g. use and retention of their location information. However, default rules should also be stated for users incapable of stating their own rules. National rules and laws must be reflected in such policies as well, and the policies can only be overridden in case of legal interception or emergency incidents. Also, the target may not necessarily be the one stating policies, e.g. parents will typically state policies regarding their child's location information. Generally, privacy can be accomplished by reducing the accuracy of the location information and by anonymity (or other non-real identities), and confidentiality by encrypting the location information.
- **Integrity** is required to prevent unauthorised modification of location information. Integrity relates to the fact that a receiver of location information should be confident that the location information received is accurate, at least to the degree of precision agreed upon with the target. The policies regulating the location information access should also be protected, so that modification of unauthorised entities is not possible. Generally, encryption and digital signatures are ways of providing integrity.
- **Availability** is required so that authorised entities are able to access the service upon demand.
- **Accountability** is required so that users can be held responsible for their actions. This is accomplished by identifying and authentication the users. Authentication will be required for all entities in a transaction involving location information to prevent impersonating.
- **Non-repudiation** is required so that evidence exist so that a target cannot deny being at a location for where it released its position. This is particularly important for legal cases.

Location information does not only increase the value of general mobile services, but will provide useful input to emergency services. As more than 50% of **emergency** calls emanate from mobile phones, it is clear that location determination is important. However, most users, or callers, is not able to determine the location very precisely in such situations, hence, the ability to provide the emergency centres with location automatically will enhance their service, and potentially save lives. In the case of an emergency, we want the location-aware service to be available, and provide short response times. Integrity is important in emergencies as we want to be sure that the location information is correctly transmitted in order to get help. Non-repudiation may be important in emergency incidents as this prevents any parties from denying the calls.

Clearly, providing location-awareness to emergency services is a good thing. However, may location-aware systems provide tools for **criminal activities**? Probably yes; new technologies tend to do so. Hence, if criminal activities are suspected, it should be possible to track individuals. This, of course, depends upon laws in the different countries, but location-aware systems should provide such an option.

It do seem as the Geopriv protocol, described in Chapter 3, will provide a secure way of transmitting location information. The Geopriv workgroup has identified three aspects that are important to secure. First, securing the Location Object (LO, which is an technology-independent object conveying location information, is important to guarantee integrity and confidentiality of the location information. It will also be important to authenticate the sender and the receiver of the LO. Second, the privacy rules play an important role towards a user's privacy and security. Finally, the ability of a user to be identified by a different identity, e.g. a pseudonym, is important to be able to provide privacy. These three areas clearly relate to the discussion provided in Chapter 4, and they seem to have captured important security requirements for provisioning of location-awareness. Also, as the Geopriv WG seeks a technology-independent protocol for transmission of their location object, this seems to be an interesting protocol for location-awareness.

5.1 Further Work

As mentioned in Chapter 1, the author has found a lot of the related work interesting (2.4.3). However, as time is limited, and undertaking such a project is a new experience, the choice was to limit the rather huge area, and look at the effort by the IETF Geopriv workgroup. The author found, however, that efforts by the Location Inter-operability Forum were interesting. LIF has stated a set of Privacy Guidelines [32], and a Mobile Location Protocol [9]. The security requirements stated by LIF do agree with the requirements stated in Chapter 4 and by the Geopriv WG. However, it could be worth looking into it. Also, effort by the Norwegian Computing Centre corresponds to the Geopriv model, as they base their security framework around having users state their own privacy policies. These efforts could be looked into for further studies.

Further, security issues relating to providing location-aware services over GSM, UMTS, GPS/GALILEO could be further investigated by looking at the technologies mentioned. [38, 39, 40, 41, 42] provides the interested reader with a few issues relating to security in 3G.

Questions

1. What are the areas that enable location-aware computing?
2. What is the aim of the IETF Geopriv workgroup?
3. What is the motivation for the attackers of Geopriv?
4. What are the three security properties of Geopriv mentioned in this paper?
5. Security requirements of location-aware mobile services can be classified under confidentiality, integrity, accountability and non-repudiation. Give a brief definition of these security terms and relate them to location information.

References

Note: (date) behind an URL indicates last date accessed.

[1] http://www.fcc.gov/911/enhanced/releases/factsheet_requirements_012001.pdf (27.11.2003)

[2] EU-112, press release IP/03/1122**:** http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.getfile=gf&doc=IP/03/1122|0|AGED&lg=EN&type=PDF (27.11.2003)

[3] Satyanarayanan, M., "Fundamental Challenges in Mobile Computing", 1996.

[4] Satyanarayanan, M., "Pervasive Computing: Vision and Challenges", IEEE Personal Communications, Aug 2001.

[5] Chapter 2: Location –Aware Computing, IT Roadmap of a Geospatial Future, http://books.nap.edu/html/geospatial_future/ch2.html (27.11.2003)

[6] Hightower, J., Borriello, G., "Location Sensing Techniques", Aug 2001.

[7] Hightower, J., Borriello, G., Location Systems for Ubiquitous Computing, IEEE Computer, August 2001.

[8] Galileo, the European Programme for Global Navigation Services, http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_brochure_march2003.pdf

[9] Location Inter –operability Forum (LIF), Mobile Location Protocol, LIF TS 101 v2.0.0.

[10] GSM Assosiation, Permanent Reference Document SE.23, Location Based Services, http://www.gsmworld.com/documents/lbs/se23310.pdf

[11] Swedberg, G., "Ericsson's mobile location solution", Ericsson Review No.4, 1999, http://www.ericsson.com/about/publications/review/1999_04/93.shtml (27.11.2003)

[12] About URIs: http://www.w3.org/Addressing (27.11.2003)

[13] Myles, G., Friday, A., Davis, N.; "Preserving Privacy in Environments with Location – Based Applications", IEEE Pervasive Computing, January – March 2003.

[14] Cuellar, J., Morris, J., Mulligan, D., Peterson, J. and Polk, J., "Gepriv Requirements", draft-ietf-geopriv-req-04 (work in progress), Oct 2003.

[15] ISO 7498-2: Information processing systems – Open Systems Interconnection – Basic Reference Model - Part 2: Security Architecture, 1989

[16] http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf (27.11.2003)

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www1.oecd.org/publications/e-book/9302011E.pdf (27.11.2003)

[18] The Platform for Privacy Preferences 1.0 Specification, World Wide Web Consortium, http://www.w3.org/P3P/ (27.11.2003)

[19] Langheinrich, M. , A Privacy Awareness System for Ubiqutious Computing Environments, http://www.inf.ethz.ch/vs/publ/papers/privacy-awareness.pdf (27.11.2003)

[20] Snekkenes, E., "Concepts for Personal Location Privacy Policies", Norwegian Computing Center, Proceedings of the ACM Conference on Electronic Commerce (EC'01), 14 -17 October 2001, Tampa, Florida, USA

[21] Fuglerud, K., Lous, J., Nordlund, B.; "A prototype for defining and enforcing privacy policies", Report, Norwegian Computing Center, ISBN 82 – 539 -0494 -0

[22] Arnesen, R., Danielsson, J., "A Framework for Enforcement of Privacy Policies", ERCIM Workshop "The role of trust in e-business", October 3rd (Subm for rev.) July 15, 2001.

[23] Aredo, D.B., Rivertz, H.J., Vestgården, J.I.; "LBS System Architecture with Privacy", Proc. of the 7th Internation Multiconference in Systemics, Cybernetics and Informatics (SCI2003) **Vol. 2003,** July 27, 2003.

[24] Danly, M., Mulligan, D., Morris, J. and Peterson, J.,"Threat Analysis of the geopriv Protocol", draft –ietf-geopriv-threat-analysis-01 (work in progress), Sept 2003.

[25] *Starner, T.E.* Wearable computers: no longer science fiction**,** IEEE Pervasive Computing, January – March 2002.

[26] Cuellar, J., Morris, J., Kanai, T., "Geopriv Scenarios and Use Cases", draft-cuellar-geopriv-scenarios-03 (work in progress), March 2003.

[27] Lopes, L., Villier, E., Ludden, B., "GSM Standards activity on location",

[28] Gollmann, D.: "Computer Security", J. Wiley & Sons, 1999.

[29] Morris, J., Mulligan, D., Cuellar, J., "Core Privacy Protection for Geopriv Location Object", draft-morris-geopriv-core-02 (work in progress), June 2003.

[30] Stallings, W.: Cryptography and Network Security, Prentice Hall, 2003

[31] http://www.trueposition.com/Press/news_05.05.03_3gpp.html (27.11.2003)

[32] http://www.3gpp.org/ftp/tsg_sa/WG3_Security/2002_meetings/TSGS3_25_Munich/Docs/PDF/S3-020478.pdf (27.11.2003)

[33] Pradhan, S.: "Semantic Location": http://www.cooltown.hp.com/dev/wpapers/semantic/semantic.asp (27.11.2003)

[34] http://www.ietf.org/html.chartes/geopriv-charter.html (27.11.2003)

[35] Sarikaya, B. (Editor), Geographic Location in the Internet (Kluwer International Series in Engineering and Computer Science, 691)

[36] Umts world http://www.umtsworld.com/technology/lcs.htm (27.11.2003)

[37] Schulzrinne, H., Tschofenig, H., Cuellar, J., Polk, J., "Policy Rules for Disclosure and Modification of Geographic Information", draft-ietf-geopriv-policy-00 (work in progress), Oct 2003.

[38] 3GPP TS 21.133 V4.1.0 (2001 -12): 3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (Release 4).

[39] 3G TS 23.271 v2.0.0 (2000-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Functional stage 2 description of LCS (Release 4)

[40] 3G TR 33.900 v0.4.1 (2001-08): 3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security (Release 5).

[41] LIF TD 201 V.3.00 (2002-2): Location Interoperability Forum; Interoperability Testing Group, The Challenge with inter-operability in LCS

[42] 3GPP TS 33.102 V6.0.0 (2003-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6).

Background Readings: (Not directly referenced)

[43] Patterson, C, Muntz, R., Pancake, C.M. ,"Challenges in Location – Aware Computing", IEEE Pervasive Computing, April – June 2003

[44] Beresford, A.R., Stajano, F.:"Location Privacy in Perasive Computing", IEEE Pervasive Computing, Jan – March 2003.

Appendix 1 **Location Sensing Systems**

Technology	Technique	Physical	Symbolic	Absolute	Relative	LLC	Recognition	Accuracy and precision if available	Scale	Cost	Limitations
GPS	Radio time-of-flight lateration	•		•		✓		1-5 meters (95-99 percent)	24 satellites worldwide	Expensive infrastructure $100 receivers	Not indoors
Active Badges	Diffuse infrared cellular proximity		•	•			✓	Room size	1 base per room, badge per base per 10 sec	Administration costs, cheap tags and bases	Sunlight and fluorescent light interfere with infrared
Active Bats	Ultrasound time-of-flight lateration	•		•			✓	9 cm (95 percent)	1 base per 10 square meters, 25 computations per room per sec	Administration costs, cheap tags and sensors	Required ceiling sensor grid
MotionStar	Scene analysis, lateration	•		•			✓	1 mm, 1 ms, 0.1° (nearly 100 percent)	Controller per scene, 108 sensors per scene	Controlled scenes, expensive hardware	Control unit tether, precise installation
VHF Omini-directional Ranging	Angulation	•		•		✓		1° radial (≈ 100 percent)	Several transmitters per metropolitan area	Expensive infrastructure, inexpensive aircraft receivers	30-140 nautical miles, line of sight
Cricket	Proximity, lateration		•	○	○	✓		4 × 4 ft. regions (≈ 100 percent)	≈ 1 beacon per 16 square ft.	$10 beacons and receivers	No central management receiver computation
MSR RADAR	802.11 RF scene analysis and triangulation	•		•			✓	3-4.3 m (50 percent)	3 bases per floor	802.11 network installation, ≈ $100 wireless NICs	Wireless NICs required
PinPoint 3D-iD	RF lateration	•		•			✓	1-3 m	Several bases per building	Infrastructure installation, expensive hardware	Proprietary, 802.11 interference
Avalanche Transceivers	Radio signal strength proximity	•			•			Variable, 60-80 meter range	1 transceiver per person	≈ $200 per transceiver	Short radio range, unwanted signal attenuation
Easy Living	Vision, triangulation		•	•			✓	Variable	3 cameras per small room	Processing power, installation cameras	Ubiquitous public cameras
Smart Floor	Physical contact proximity	•		•			✓	Spacing of pressure sensors (100 percent)	Complete sensor grid per floor	Installation of sensor grid, creation of footfall training dataset	Recognition may not scale to large populations
Automatic ID systems	Proximity		•	○	○		✓	Range of sensing phenomenon (RFID typically <1m)	Sensor per location	Installation, variable hardware costs	Must know sensor locations
Wireless Andrew	802.11 proximity		•	•			✓	802.11 cell size, (≈ approx. 100 m indoor, 1 km free space)	Many bases per campus	802.11 deployment, ≈ $100 wireless NICs	Wireless NICs required, RF cell geometries
E911	Triangulation	•		•			✓	150-300 m (95 percent)	Density of cellular infrastructure	Upgrading phone hardware or cell infrastructure	Only where cell coverage exists
SpotON	Ad hoc lateration	•			•		✓	Depends on cluster size	Cluster at least 2 tags	$30 per tag, no infrastructure	Attenuation less accurate than time-of-flight

Tabell 1-A Location Sensing Systems [5]

Appendix 2 Positioning Methods

This section provides the interested reader with a brief overview on how to location information is determined in GSM and in UMTS.

2.1 Determining location in GSM

The Mobile Location Centre (MLC) in GSM is responsible for a set of task such as privacy, authorisation and authentication, delivery of location information to authorised applications, billing and charging, access to base station coordinates and other physical parameters required for location, and the calculation of the final location estimate based on received signal measurements from either the handset or the base station. The figure below shows an overview of the GSM Location Network Architecture.

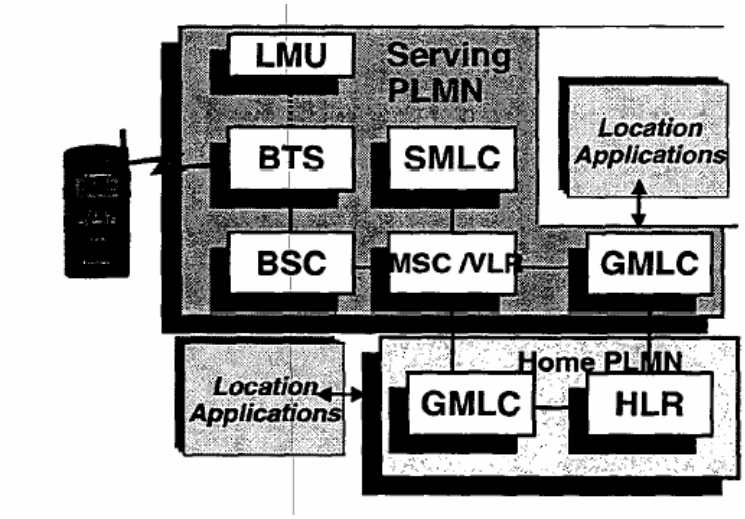


Figure 2-A: GSM Location Network Architecture [27]

The MLC can be either Serving MLC (SMLC) or a Gateway MLC (GMLC), which interfaces to external applications. The GSM Location Network Architecture also contains a network element known as the Location Measurement Unit (LMU), which is used to provide physical measurements required for the location estimation. The function of this unit, however, depends on the method of location being deployed. There are a couple of location methods in GSM. These position methods will be described briefly in this section. [10] divide positioning technologies into three categories: basic, enhanced and advanced, as shown in the table below.

Level	*Method*	*Handset dependence*
Basic	CI, CI+TA, CI+TA+RX	No
Enhanced	E-OTD, TOA	Yes/No
Advanced	A-GPS	Yes

Tabell 2-A: Position Methods in GSM [10].

It is also possible to differentiate between terminal–based (handset–based) and network–based positioning methods [11]. A terminal–based positioning solution relates to intelligence in the terminal or its SIM card. Hence, it requires the customer to buy a new terminal, a new SIM card or possibly both, to benefit from the location system. The networked–based positioning solution, however, do not require intelligence to be built into the mobile terminal. This way, the market penetration will be 100% from the day the service is launched.

Terminal –based solutions

This section looks at two terminal based positioning methods: A–GPS and E–OTD. As mentioned, there are a few drawbacks to the GPS. However, the GSM network can provide assistance information that can give better coverage than stand–alone GPS receivers. This position method - *Assisted GPS (A GPS)* - is a time based method, where the handset measures the arrival time of signals transmitted from three or more GPS satellites. An illustration is provided below.

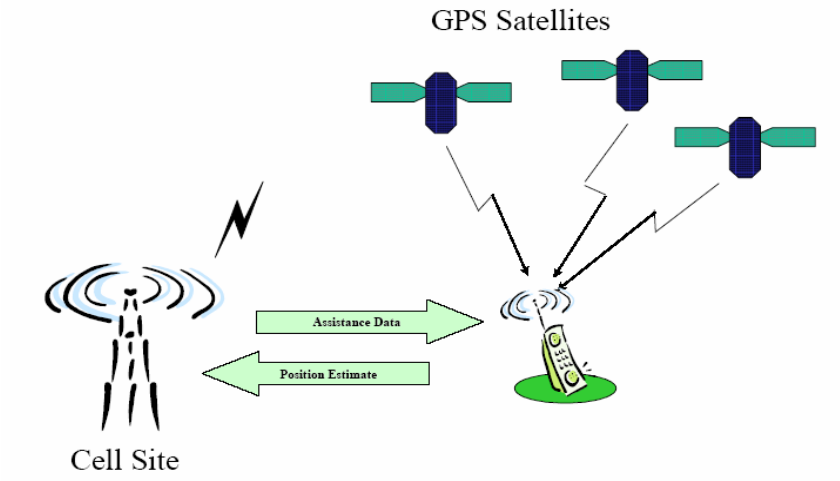


Figure 2-B: Assisted GPS [10]. The handset measures arrival time of signals transmitted from three or more GPS satellites.

Another time–based position method is the *Enhanced Observed Time Difference (E –OTD)*. The handset measures the arrival time of signals transmitted from three or more Base Transceiver Stations (BTSs). The position is determined using triangulation based on the distance returned from each BTS to the Mobile Station (MS). The E- OTD method can be either handset –assisted or handset–based. In the handset–assisted the timing measurements made by the handset are transferred to the SMLC using standardized signalling, whereas in the handset–based , the position calculation function is in the handset, and the position is then returned to the SMLC. An illustration of the E–ODT method is provided in Figure 2-C. Triangulation is done either by lateration, which uses multiple distance measurements between known points, or via angulation, which measures angle or bearing relative to points with known separation.

In UMTS the similar method is called OTDOA – IPDL (Observed Time Difference Of Arrival – Idle Period Down Link). For illustration, see section 2.2 in this appendix.

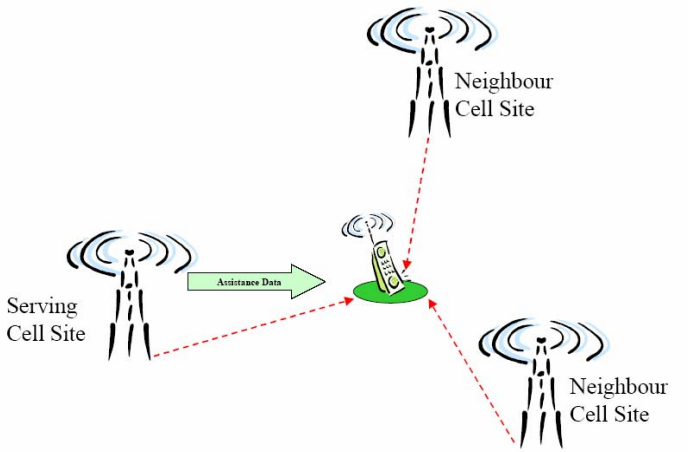


Figure 2-C E–OTD [10] The handset measures the arrival time of signals transmitted from three or more Base Transceiver Stations (BTS), and estimates position using triangulation.

Network –based solutions

This section looks at two different ways of determining position in the GSM networks. The first and most basic positioning method is based on the use of the *cell identification*. This cell id is converted to a geographic position using knowledge of the operator's network. Hence, accuracy is dependent on the cell size, and may not be very accurate. Timing Advance (TA) can be used to improve performance if available. Figure 2-D below shows an illustration of the cell id position method. Another method, The Uplink time of arrival (UL–TOA), is based on measuring the time of arrival of a signal from a mobile terminal to four or more measurement units (LMU).

In order for the location services to work effectively outside the home network, terminals and the visited network must support the same positioning method. For services based on cell ID, this is not an issue. However, for services based on E–OTD, OTDOA or A–GPS, it cannot be assured that the service will be available whilst roaming. Hence, as mentioned earlier, interoperability is important.

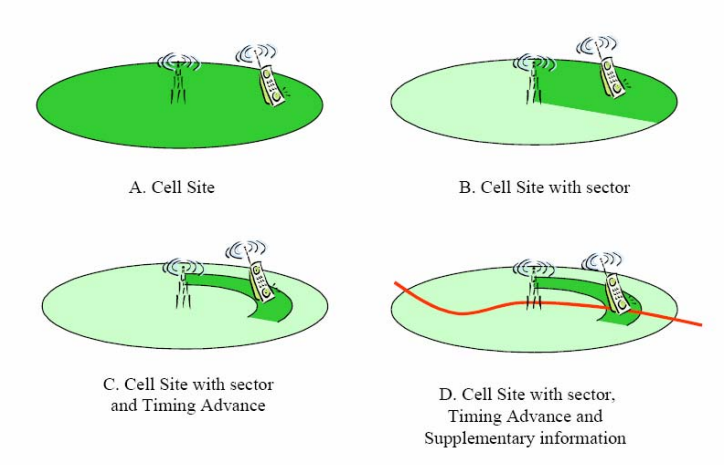


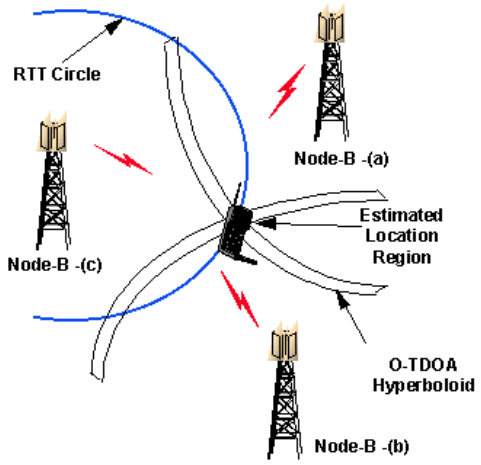
Figure 2-D: The Cell ID position method [10].

2.2 Determining location in UMTS

The 1999 release specification specifies the following positioning methods:

- Cell based positioning method
- Observed Time Difference Of Arrival (OTDOA) method with network configurable idle periods [31].
- Assisted GPS methods

An illustration of the OTDOA method is provided below.



Figur 2-E: The OTDOA Location Method [36]

Each OTDOA measurement for a pair of downlink transmissions describes a line of constant difference (a hyperbola) along which the mobile phone may be located. The mobile phone's position is determined by the intersection of these lines for at least two pairs of Node Bs. The accuracy of the position estimates made with this technique depends on the precision of the timing measurements, the relative position of the Node Bs involved, and is also subject to the effects of multipath radio propagation.

Appendix 3 Geopriv Scenarios

This section aims at providing the reader with a few scenarios in Geopriv, to better understand the Geopriv concepts. Towards the end, a summary of privacy issues identified by the scenarios are summarized.

In many of the scenarios that we will consider, an entity will take on different roles. In some cases, the RM and the Target are the same entity (individual), in some cases they are not. The Target may also be a LG if the Target device it self is capable of computing the location. Also, depending on the device capabilities, the device may serve as a LS. If not, the Target will have to rely on an external LS. To better understand some of these concepts introduced, I will look at a few scenarios in the following section.

How the computing process is done also give raise to different scenarios. Generally, the location computing process contains the following two steps [26]:

- Obtaining the raw data about the Target's location.
- Deriving or computing the Target's location using this raw data.

This in turn raises two questions that lead us to different scenarios. First, who has control over the raw data? The answer to this question might be i) the Target's device, or ii) the Target's Access Provider (AP). And then finally, who has control of the location computation? This may be the Target's device, the Target's AP or a 3rd party. One potential illustration of the different abstract scenarios is shown below in Figure 3-A. From a privacy (security) point of view, it is important that the entities that have access to the raw data comply with the privacy rules set by the RM.

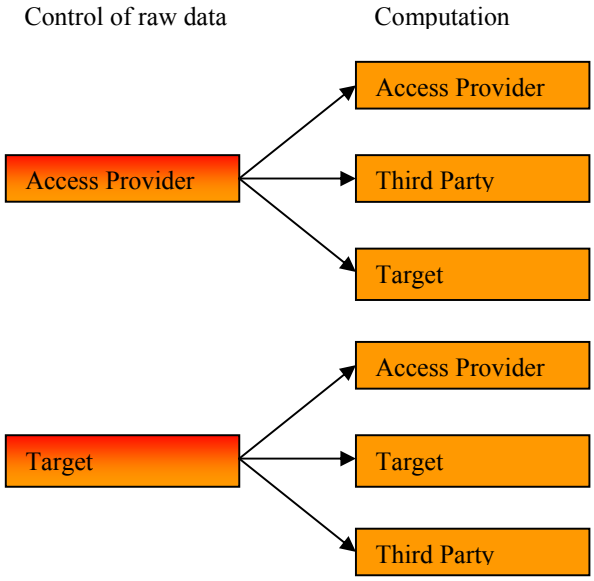


Figure 3-A: Who controls the raw data, and who controls the location computation? This figure illustrates the different possibilities. It is important that security/privacy is maintained in all entities.

This section proceeds by looking at the following scenarios sets:

- Where am I? The target seeks its own location.
- Where is he/she?
- Complex scenarios.

3.1 Where am I?

In the first, rather simple, scenario to be considered, the target wishes to find out its position using the Global Positioning System (GPS) (see section 2.1.3). The device itself is also capable of processing the raw data obtained to determine its location. In this scenario, the GPS enabled device receives transmissions from the GPS satellites, computes and displays the current location of the device. As no external entity is granted access to location information –it is a *closed system* - this minimizes privacy concerns. However, as the device can be lost, stolen and possibly accessed through legal processes, there are issues about data retention and data security that must be solved.

Another possible scenario to consider is where the GPS enabled device has no internal computing power, so that the location information must be computed elsewhere using the raw GPS data. This scenario is depicted in Figure 3-B.

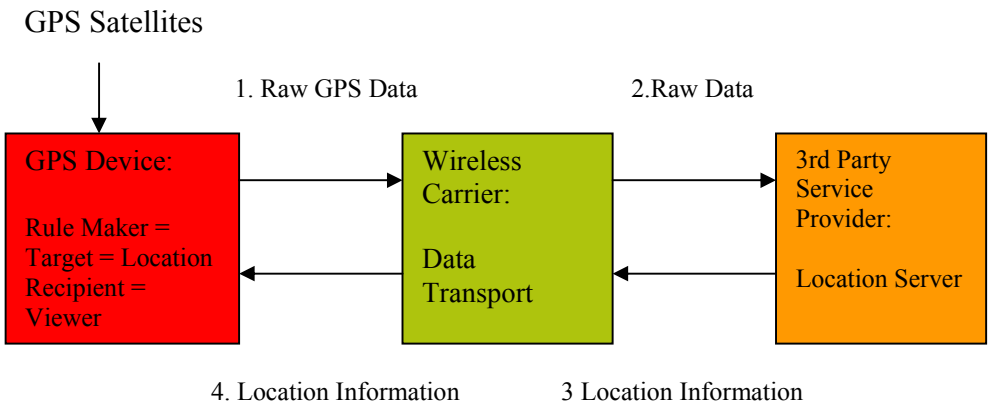


Figure 3-B: Where am I? Target seeking location information using GPS Device with NO internal computing power [26].

Here, the device receives raw GPS location data, and sends it, via the wireless carrier network, to a third party LS. The LS then processes the data, and sends it back to the device. Depending on privacy rules set by the target (or RM), the LS may or may not store the location information. The security concerns mentioned in the last scenario still remain valid, and some additional concerns are raised. For example, we need to make sure that the information sent via the wireless carrier is secured. We also need to make sure that the information can not be reused (replayed), and consider security issues that raises from the fact that the location information may be stored.

Other possible scenarios include the one where the target does not carry a GPS enabled device, and therefore have to ask the wireless carrier for its position. Then the wireless carrier would be a LG and a LS in addition to just being a data transporter.

3.2 Where is he/she?

Now, let us consider a few scenarios where a 3rd party seeks location of a target. Again, we will first look at a scenario where the target device has computing power, and location awareness. For illustration of this see Figure 3-C.

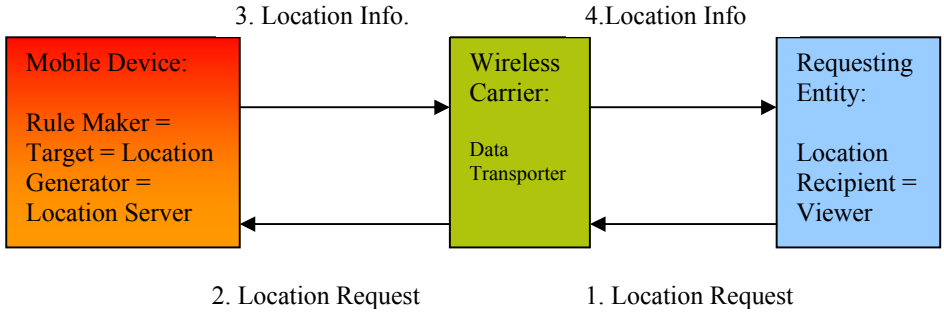


Figure 3-C: Where is he/she? A third party seeking location information about a target with device with computing power and location awareness [26].

In this case, the LR seeks the position of the mobile target device. The location request is sent to the application running on the target. The application then authenticates the LR, and then checks if the rules allow for release of position, then transforms the location information according to the rules if necessary, and sends the filtered location information back to the LR. Here, the rules are only internal to the target; hence, they need not be standardized. The LR, however, must obey the rules. The rules may be conveyed or referenced in the Location Object.

Next, a similar scenario will be discussed. Here, the target being located has a device with computing power, but no location awareness. This scenario is shown in Figure 3-D.

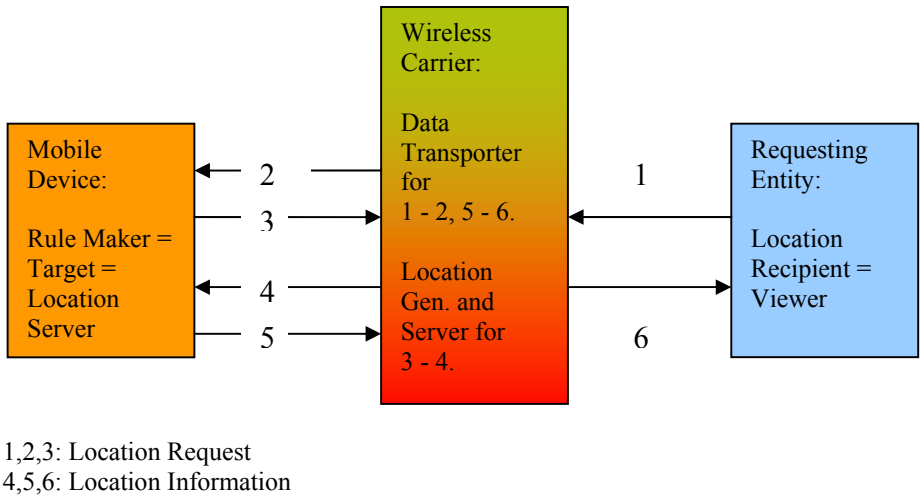


Figure 3-D: Where is he/she? A third party seeking location information about a target with device with computing power, but no location awareness.

In this scenario the mobile device requests the wireless carrier to determine the location of the device and send it back to the mobile device. The mobile node sends this location information to the requesting entity. Privacy concerns include questions on how the RM can make sure that the LG does not provide this location information to other LRs, and how to authenticate the supplied location information. Once again, it is clear that the entities must be aware of the rules set by the owner, or obeys some default rules, i.e. set by laws, contract or the protocol. Also, in such tracking scenarios, the privacy of "unintended targets" must be considered. An unintended target

is, for example, the person who rented a car from a car rental company. This person will implicitly be tracked, when the car rental company tracks the car.

3.3 More complex scenarios

This section looks into two more complex scenarios as provided by [26]. The first scenario the target itself has a location aware device, but is using a 3rd party location server to obtain LBS from a 4th party SP. An illustration is provided in Figure 3-E..

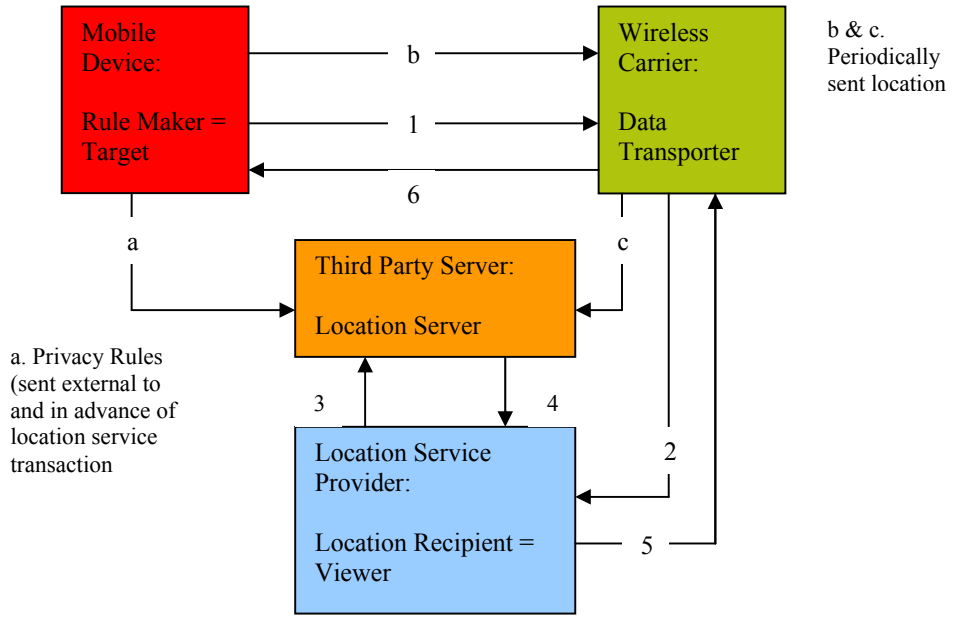


Figure 3-E: Target with location aware device using a third party location server to obtain location based services from a fourth party service provider.

Here, the mobile device, which acts as a Target, the RM and the LG, knows or discovers its own position, i.e. by using GPS or manually inputting position. This position information is periodically sent to a 3rd party Location Server. There exist a prior contractual agreement between the Target and the LS, and the Target sends the LS its privacy rules in advance. Then, when the Target seeks a location server, it requests this from the service provider, which in turn requests the information from the LS, and then fills the request for service.

In scenario number two the target's device is not location aware, so it needs to obtain the location information from the wireless carries. Otherwise, the scenario is the same. An illustration is provided in Figure 3-F.

Here, the Target's device does not know its location. Rather, its LS must ask the Targets wireless carrier (Access Provider). This way, the wireless carrier acts as a Location Server who provides the initial position information.

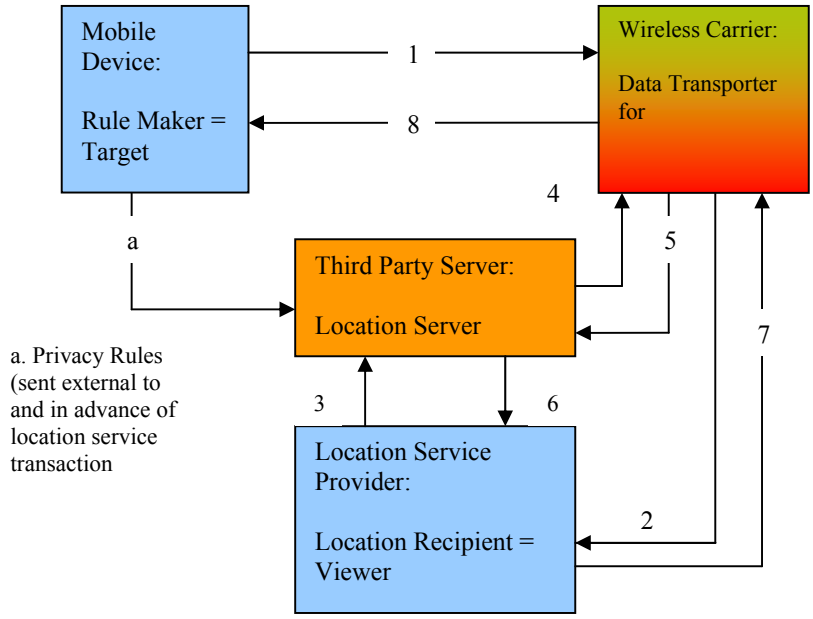


Figure 3-F: Target with a device that is not location aware using a third party location server to obtain location based services from a fourth party service provider.

3.4 Privacy issues shown by the scenarios

By looking at the scenarios provided, we notice that all scenarios, except the first one (being a closed system), presents some kind of privacy issues. Hence, we have to have a clear agreement and understanding of the following questions:

- Who controls the data?
- How is the data controlled?
- Who computes and derives the location information?
- Who stores, uses and discloses the data?

These issues can be solved by setting out a set of clear –cut rules, and by obeying rules. Contractual agreements are also a possibility. The Geopriv protocol suggests the use of the Geopriv Location Object as a way of allowing "a Rule controlled disclosure of location information for location services". The information in the LO is secured according the rules set by the RM, but other objects or headers are in general not secured in the same way. Hence, some forms of traffic analysis will still be possible.

The security properties of the Geopriv are described in section 3.3.