Chapter 15

Privacy-Enhanced Location Services

Claudio A. Ardagna, Marco Cremonini, Ernesto Damiani, Sabrina De Capitani di Vimercati, and Pierangela Samarati

Contents

15.1 Introduction

In today pervasive environments, access to location information is achieved through a variety of sensor technologies, which recently enjoyed a relevant boost in terms of precision and reliability, and through the widespread diffusion of mobile communication devices. Location information is therefore becoming easily available and can be processed to provide services for business, social, or informational purposes [1]. In particular, location

information allows the development of a new category of applications, generally called *location-based services* (LBSs), which use the physical position of individuals to offer additional services. For instance, customer-oriented applications, social networks, and monitoring services can be greatly enriched with data describing where people are, how they are moving, or whether they are close to specific locations. Several commercial and enterprise-oriented LBSs are already offered and have gained popularity [2,3]. However, despite the tremendous success of mobile computing, as witnessed by the exponential growth of advanced mobile devices like smart phones and handheld computers, location-based computing also brings a number of privacy concerns. It is not a surprise that personal privacy, which is already the center of many concerns for the risks brought by current online services [2,4], is considered seriously threatened by LBSs. Such concerns call for more sophisticated solutions for preserving the privacy of users when dealing with location information.

In addition, the publicity gained by recent security incidents that have targeted the privacy of individuals has focused the attention of the media and revealed faulty data management practices and unauthorized trading of personal information of users (including ID thefts and unauthorized profiling). For instance, some legal cases have been reported, when rental companies used GPS technology to track their cars and charge users for agreement infringements [5], or when an organization that used a "friend finder" service to track its own employees [6]. Furthermore, research on privacy issues has gained a relevant boost since providers of online and mobile services, often largely exceeded in collecting personal information as a requirement for service provision. In this context, the protection of location privacy of the users is today one of the hottest and most critical research topics.

Interestingly, privacy issues in online services have been analyzed from different perspectives and by several scientific disciplines. Many sociological studies of the privacy problem [2,7] have been conducted to reach a better understanding of the concerns perceived by users in adopting a location-based service. In particular, Barkhuus and Dey [2] present an experimental case analyzing location privacy concerns and how they are related to a service nature and characteristics. The study is focused on *location-tracking services*, where locations of users are tracked by third parties, and on *position-aware services*, where mobile and portable devices are aware of their own position. The result of this research, which examined a location-tracking service and a position-aware service, is that users perceived the latter as more respectful of their privacy and, therefore, were more likely to subscribe to it rather than to the location-tracking service. However, although location-tracking services are considered more critical with respect to privacy, they represent a promising application class

that could have a large success, if users were provided with a simple and intuitive means to protect their location privacy.

From a technological point of view, most of the current research on LBS privacy focuses on providing anonymity or support for partial identities to online and mobile services that do not require the personal identification of a user for their provision [8–11]. Although important, anonymity or partial identification are not always viable options for the provision of online services [12,13]. To a certain extent, anonymity and complete knowledge of location information are the opposite endpoints of all possible degrees of knowledge of personal information bound to identities. Location information is just one class of personal information that sometimes can be associated with anonymous entities, but that often must be bound to user identity. When identification of users is required and, consequently, anonymity is not suitable, a viable solution to protect users privacy is to decrease the accuracy of personal information bound to identities [14–16]. For several online services, in fact, personal information associated with identities does not need to be as accurate as possible to guarantee a certain service quality. This is often the case of location-based information that, in many real applications, can be dealt with suboptimal accuracy levels while offering an acceptable quality of service to the final users.

In this chapter, we review the main techniques used for protecting the location privacy of users in online services. The remainder of this chapter is organized as follows. Section 15.2 discusses the basic concepts of current positioning systems and of location-based services. Section 15.3 provides an overview of the location privacy issues discussing different categories of location privacy that must be preserved depending on the scenarios and on the requirements. Section 15.4 presents some techniques that can be used to protect location privacy, analyzing their characteristics and applicability. Finally, Section 15.5 presents our conclusions and an outline of future research directions.

15.2 Basic Concepts and Scenario

Recent enhancements in positioning technologies have been fostering the development of many location-based services that guarantee a high quality of service in any environment. Figure 15.1 illustrates a typical scenario where a user submits a request to a location-based service and the service provider interacts with a positioning system to obtain the user location. Before analyzing the main location privacy issues, we review some of the existing positioning technologies and introduce some notable location-based services based on them.

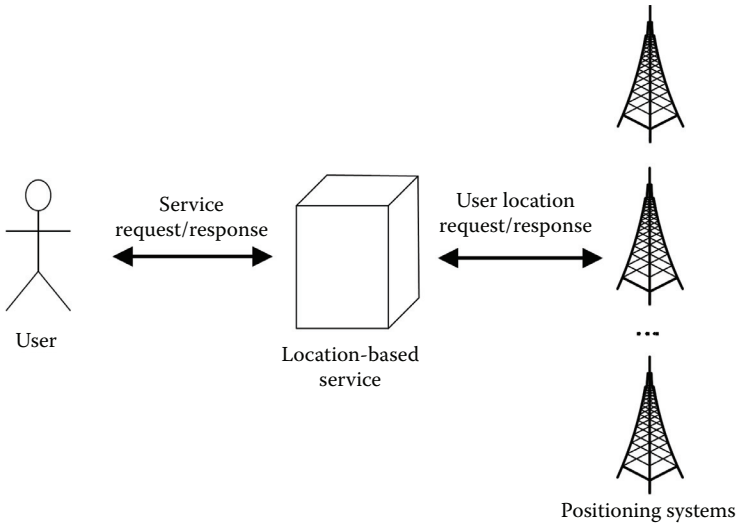

Figure 15.1 Basic scenario.

15.2.1 Positioning Systems

Positioning systems measure the location of users carrying mobile devices. Several location technologies (e.g., GSM/3G technology, GPS, WiFi, and RFID) have been developed to compute location information, each enjoying a relevant boost in terms of precision and reliability. Performance-related properties (e.g., quality of service) of a location service largely depend on the underlying technologies. Technologies like 802.11 WiFi and AGPS/GPS [17,18] can be exploited, even if their applicability is limited. WiFi, for example, has a limited coverage and its usage is restricted to indoor environments (e.g., buildings, airports, malls) and urban areas covered by hotspots. By contrast, GPS does not work indoors, or in narrow spaces; however, it has no coverage limitation, a feature that makes it an ideal location technology for open, outdoor environments.

The improved location capabilities of GSM/3G technologies and the widespread adoption of their mobile devices make GSM/3G positioning systems the most suitable technology for the delivery of services based on physical locations of users. For service provisioning, the location-based service collects the user location by querying one or more positioning systems. Today, most people always carry a mobile phone, a habit that makes it straightforward to gather their location position. Also, several location techniques have been studied and developed for achieving a good level of performance and reliability in any environment with few limitations.

Among the techniques used by GSM/3G technology for location purposes, the most important and already standardized are the following.

- *Cell Identification*. This is the simplest technique and is based on the identification of the mobile terminal serving cell. The spatial coordinates of the cell provide a broad estimation of a user position, which depends on the radius of the cell, where the radius can be between 200 m and 2.5 km. In urban areas, cells are much smaller than in the countryside.
- *Signal Level*. This measures the signal attenuation between the mobile terminal and the base station to calculate a user's position. Unless advanced and computationally heavy ray-tracing algorithms are used, the signal level technique is not well-suited for indoor or urban areas.
- *Angle of Arrival (AoA)*. This assumes that more than one single base station for signal reception is available. A user's position can be calculated by computing the angle of arrival at two base stations. It should be noted, however, that if there is no line-of-sight between the mobile terminal and the base stations, the calculated angles do not correspond with the actual directional vector from the base stations to the mobile.
- *Time of Arrival (ToA)*. This calculates the distance between a base station and a mobile phone by measuring the time for a signal to complete a round trip between the two endpoints. Signal arrival can be delayed by walls or natural obstacles, decreasing location accuracy.
- *Time Difference of Arrival (TDoA)*. This computes the time difference between station-to-terminal propagation, with the purpose of increasing the location accuracy. It can be realized by measuring the differences of arrival time of a certain burst sent by the mobile to several base stations or by recording the time differences of impinging signals at the mobile.

Several papers describe and discuss different location technologies and the best accuracy that can be achieved [19,20], observing, in particular, that technological improvements in positioning systems can reduce a location error to a few meters, regardless of the particular environment (e.g., urban, suburban, rural, outdoor, or indoor). This location accuracy of sensing technology, combined with the widespread diffusion of GPS, WiFi, and cellular phones, calls for an urgent and careful consideration of users privacy concerns. Such concerns are even more critical if we consider that user mobile devices are not able to define restrictions on location data scattering or to stop the data flow (unless the mobile devices are switched off). The worst-case scenario that some analysts have foreseen as a consequence of

an unrestricted and unregulated availability of location technologies recalls the well-known "Big Brother" stereotype: a society where the secondary effect of location technologies, whose primary effect is to enable the development of innovative and useful services, is a form of implicit total surveillance of individuals.

15.2.2 Location-Based Services

The great amount of location information now available gives a considerable boost to location-based services development and deployment. The research efforts result in the definition of many location-based services for business, social, or informational purposes [21]. There are different types of location-based services, as listed below.

- *Nearby-Information Services.* These provide information about the environment surrounding the location of a user (e.g., point of interest, advertisement, or weather and traffic alerts). A user, after subscribing to these services, receives real-time information through a mobile device.
- *"Locate-Me" Services.* These give information about the position of users. They should be used when authorized third parties need to know positions of users. In particular, a locate-me service is well suited for location-based access Control (LBAC) services that use the location of users to evaluate and enforce access requests submitted by the users themselves [22].
- *Tracking Services.* These offer information about user movements, such as her path when entering or leaving some areas, her velocity, direction, and so on. It could be used by online services that provide vehicles tracking, tracking of children or employees, warning about dangerous areas, and so on.
- *Locate-Friends and Nearby-Friends Services.* These give information to subscribers about the real-time location or proximity of other subscribers. They could be used, for example, to provide services in the context of social networks.
- *Personal-Navigator Services.* These provide information about the path that has to be followed to reach a target location from the current user's location. The services rely on tracking services to gather the position of a user moving on the field.

The cost of integrating location technologies in existing telecommunication infrastructures can be economically sustained by most companies. Many projects offering locate-me, locate-friends, tracking, personal-navigator, or nearby-information services have been developed. Examples of such projects are *"Teen Arrive Alive"* [23], *uLocate* [24], *CellSpotting* [25],

and *Mologogo* [26]. In addition, many other services have been developed, for example, for touristic purposes, such as *Guide Project* [27] that provides tourists with context-aware tourist guides, for children, or for elderly safety [28].

To conclude this brief description of the main application areas that are currently exploiting location technologies, it is important to highlight that LBSs can be useful in critical contexts, where the availability of a precise location can help in protecting human live. For instance, operators, like the enhanced 911 in North America [29], can immediately dispatch emergency services (e.g., emergency medical services, police, or firefighters) where they are needed, reducing the margins of error.

15.3 Location Privacy

User privacy has been considered a fundamental right, internationally recognized in Article 12 of the United Nations Universal Declaration of Human Rights [30]. In particular, location privacy can be defined as the right of the users to decide how, when, and for which purposes their location information could be released to other counterparts. Location privacy receives much consideration due to the exponential availability of reliable location technologies and location-based services. In this context, privacy issues have gained great relevance only recently.

Failure in protecting the location privacy of users could be exploited by malicious users to enforce different attacks such as [31]:

- Unsolicited advertising of products and services available nearby users position
- Physical attacks or harassment
- Users profiling and inferences of personal information, such as state of health, point of interests, hobbies, and so on

Location privacy can assume several meanings and pursue different objectives, depending on the scenario in which the users are moving and on the services with which the users are interacting. Location privacy protection can be aimed either at preserving the privacy of the user identity, the single user location measurement, or the location movement of the user monitored in a certain period of time. The following categories of location privacy can then be identified.

- *Identity privacy*. The main goal is to protect users' identities associated with or inferable from location information. For instance, many online services provide a person with the ability to establish a relationship with some other entities without her personal identity

being disclosed to those entities. In this case, the best possible location measurement can be provided to the others entities, but the identity of the users must be preserved.

- *Position privacy.* The main goal is to perturb locations of the users to protect the positions of individual users. In particular, this type of location privacy is suitable for environments where users' identities are required for a successful service provisioning. An example of a technique that most solutions either explicitly or implicitly exploit consists of scaling a location to a coarser granularity (e.g., from meters to hundreds of meters, from a city block to the whole town, etc.).
- *Path privacy.* The main goal is to protect the privacy of the users who are monitored during a certain period of time. The location-based services will no longer receive a single location measurement, but they will gather many samples allowing them to track users. In particular, path privacy can be guaranteed by adapting the techniques used for identity and position privacy to preserve the privacy of a user who is continuously monitored.

These categories of location privacy pose different requirements that are guaranteed by different privacy technologies, which we will analyze in the following section. Note that no technique is able to provide a general solution satisfying all the privacy requirements.

15.4 Techniques for Location Privacy Protection

With respect to the different categories of location privacy described in section 15.3, we describe the main location privacy protection techniques that can be classified as anonymity-, obfuscation-, and policy-based. In particular, anonymity-based and obfuscation-based techniques are dual categories. While anonymity-based techniques have been primarily defined to protect identity privacy and are less suitable for protecting the position privacy, obfuscation-based techniques are well-suited for position protection and less integrable with identity protection. Regarding path protection, both anonymity-based and obfuscation-based techniques are well-suited and able to provide the required degree of protection. Nevertheless, more studies and proposals have been focused on anonymity-based rather than on obfuscation-based techniques. Concerning policy-based techniques, at first sight, they can seem the most suitable solution because they are more flexible and, in general, well-suited for all the location privacy categories. However, policy-based techniques can be difficult to understand and manage for end users.

15.4.1 Anonymity-Based Techniques

An important line of research in location privacy protection relies on the notion of *anonymity* [8–11]. Anonymity typically refers to an individual, and it states that an individual (i.e., the identity or personally identifiable information of an individual) should not be identifiable.

Beresford and Stajano [8,32] propose a method called *Mix zones* that uses an anonymity service based on an infrastructure that delays and reorders messages from subscribers within predefined zones. The Mix zone model is based on the concepts of *application zone* and *Mix zones*. An application zone represents homogeneous application interests in a specific geographic area, while a Mix zone represents an area where a user cannot be tracked. In particular, within Mix zones, a user is anonymous in the sense that the identities of all users coexisting in the same zone are mixed and become indiscernible. The Mix zone model is managed by a trusted middleware that lies between the positioning systems and the third party applications and is responsible for limiting the information collected by applications. Furthermore, the infrastructure makes a user entering the Mix zone unlinkable from other users leaving it. The authors also provide an analysis of an attacker behavior by defining and calculating the *anonymity level* assured to the users, i.e., the degree of privacy protection in terms of uncertainty. They show that the success of an attack aimed at recovering users identities is an inverse measure of the anonymity provided by the privacy service.

The authors argue that an attacker aiming to reduce the anonymity level within a Mix zone can determine the mapping between ingress and egress paths that exhibit the highest probability. It is also necessary to measure how the probability of the selected mapping varies when this mapping is compared with all the other possible mappings. The anonymity level is then calculated by measuring the level of *uncertainty* of the selected mapping between inbound and outbound paths. The uncertainty is computed through traditional Shannon's entropy measure [33]. If the entropy is equal to b bits, 2^b users are indistinguishable. Also, a lower bound to the level of anonymity of a user u is calculated as the level of anonymity provided by assuming that all users exit the Mix zones from the location that has the highest probability. To conclude, the Mix zones model is aimed at protecting long-term user movements while still allowing the interaction with many location-based services. However, Mix zones effectiveness is strongly dependent on the number of users joining the anonymity service and, in particular, on the number of users physically co-located in the same Mix zone at the same time.

Bettini et al. [9] discuss privacy issues raised by a location-based service scenario. Their paper proposes a framework able to evaluate the risk

of sensitive, location-based information dissemination, and introduces a technique aimed at supporting *k*-anonymity [15,16]. The concept of *k*-anonymity tries to capture a traditional requirement followed by statistical agencies according to which the released data should be indistinguishably related to no less than a certain number (*k*) of users. Traditionally, *k*-anonymity is based on the definition of *quasi-identifier*, which is a set of attributes exploitable for linking. The *k*-anonymity requirement then states that each release of data must be such that every combination of values of quasi-identifiers can be indistinctly matched to at least *k* individuals.

The proposal in [9], therefore, puts forward the idea that the geolocalized history of the requests submitted by a user can be considered as a quasi-identifier that can be used to discover sensitive information about the user. For instance, a user tracked during working days is likely to commute from her house to the workplace in a specific time frame in the morning and to come back in another specific time frame in the evening. This information could be used to reidentify the user. In the framework proposed in [9], based on the concepts of quasi-identifier and historical *k*-anonymity, the service provider, which gather both the users' requests for services and the sequence of updates to users' locations, should never be able to link a subset of requests to a single user. To make this possible, there must exist *k* users having a personal history of locations *consistent with* the set of requests that has been issued. Intuitively, a personal locations history of a user is consistent with a set of service requests when, for each request, there exists a location in the personal history of locations where the user could have made the request. The kind of solution is highly dependent on the actual availability of indistinguishable histories of locations: If *k* indistinguishable histories do not exist, *k*-anonymity cannot be preserved. The worst case scenario is when a given user has a history different from all the others, meaning that the user cannot be anonymized and she is always identifiable.

Other works [10,11] are based on the concept of location *k*-anonymity, meaning that a user is indistinguishable by other $k-1$ users in a given location area or temporal interval. Gruteser and Grunwald [11] define *k*-anonymity in the context of location obfuscation. They propose a middleware architecture and an adaptive algorithm to adjust location information resolution, in spatial or temporal dimensions, to comply with the specified anonymity requirements. To this purpose, the authors propose the concepts of *spatial* and *temporal cloaking* used to transform a user's location to comply with the requested level of anonymity. Spatial cloaking guarantees the *k*-anonymity required by the users by enlarging the area where a user is located until the area contains *k* indistinguishable users. The same reasoning could be applied to temporal cloaking, which is an orthogonal process with respect to the spatial one. Temporal cloaking could provide spatial coordinates with higher accuracy, but it reduces the accuracy in time.

The key feature of the adaptive cloaking algorithm is that the required level of anonymity can be achieved for any location.

Gedik and Liu [10] describe another *k*-anonymity model aimed at protecting location privacy against various privacy threats, and provide a framework supporting location *k*-anonymity. Each user is able to define the minimum level of anonymity and the maximum acceptable temporal and spatial resolution for her location measurement. A message perturbation engine provides location anonymization of request messages sent by users through identity removal and spatio-temporal obfuscation of location information. This engine is composed of four major components that process each incoming message: (1) the *zoom-in component* identifies all pending messages, (2) the *detection component* identifies the *k* messages that can be used in the anonymization process, (3) the *perturbation component* applies a perturbation algorithm on messages identified by the detection component and forwards the generated messages to the location-based service, and (4) the *expiration component* deletes all expired messages. The suitability of this method depends on the number of messages received by the location protection component, which is responsible for message perturbation, and on the message expiration. If the expiration timeout is too short, many messages will be dropped; if it is too long, many useless messages will be processed. A drawback common to all solutions based on *k*-anonymity is that their applicability and performances depend on the number of users physically located in a particular area.

Another line of research that relies on the concept of anonymity is aimed at protecting the *path privacy* of the users [34–36]. In particular, path privacy involves the protection of users that are continuously monitored during a time interval. This research area is particularly relevant for location tracking applications designed and developed for devices with limited capabilities (e.g., cellular phones), where data about users moving in a particular area are collected by external services, such as navigation systems, which use them to provide their services effectively. Gruteser et al. [34] propose a solution to path privacy protection by means of path anonymization. A path is anonymized by associating a pseudonym with a user's location. However, an attacker that gains access to this information is able to associate a path and a pseudonym with a single user by looking at path information, such as the place in which the user stays during the night. To the purpose of strengthening the anonymity, multiple pseudonyms, which change over time, can be associated with a single user. The authors also argue that it is difficult to provide strong anonymity for path protection because it would require the existence of several users traveling along the same path at the same time, an assumption that often cannot be satisfied in a real-world scenario. Hence, Gruteser et al. provide two techniques for weaker anonymity: *path segmentation* and *minutiae suppression*. With weaker anonymity, users could potentially be linked to their identities,

but this requires huge efforts. Path segmentation partitions a user's path into a set of smaller paths, and at the same time changes the associated pseudonym. Path segmentation is usually implemented by defining a segment duration and mean pause. After the segment duration time, location updates are suppressed for the given pause period. Minutiae suppression suppresses instead those parts of a path that are more distinctive and could bring an easy association between a path and an identity. The suitability of these techniques is highly dependent on the density of users in the area in which the adversary collects location samples. In areas with low density of users, an adversary has a good likelihood of tracking individuals, whereas in areas with many overlapping paths, linking segments to identities can be extremely difficult.

Other relevant works consider path protection as a process whose outcome must be managed by a service provider. To this aim, privacy techniques also have to preserve a given level of accuracy to permit a good quality-of-service provisioning. Gruteser and Liu [35] present a solution based on the definition of a *sensitivity map* composed of sensitive and insensitive zones. The work defines three algorithms aimed at path privacy protection: *base*, *bounded-rate*, and *k*-area. The *base* algorithm is the simplest algorithm; it releases location updates that belong to insensitive areas only, without considering possible inferences made by adversaries. The *bounded-rate* algorithm permits the customization of location updates frequency to reduce the amount of information released near a sensitive zone and to make the adversary process more difficult. Finally, the *k*-area algorithm is built on top of sensitivity maps that are composed of areas containing *k* sensitive zones. Location updates of a user entering a region with *k* sensitive areas are temporarily stored and not released. If a user leaving that region has visited at least one of the *k* sensitive areas, location updates are suppressed, otherwise they are released. Experiments show that the *k*-area algorithm gives the best performance in terms of privacy, also minimizing the number of location updates suppression. Ho and Gruteser [36] introduce a path confusion algorithm. This algorithm is aimed at creating cross paths of at least two users. In this case, the attacker cannot recognize which path has followed a specific user.

In summary, anonymity-based techniques are suitable for all those contexts that do not need knowledge of the identity of the users.

15.4.2 Obfuscation-Based Techniques

Obfuscation is the process of degrading the accuracy of the location information to provide privacy protection. Different from anonymity-based techniques, the main goal of obfuscation-based techniques is to perturb the location information still maintaining a binding with the identities of users.

Duckham and Kulik [14] define a framework that provides a mechanism for balancing the individual needs for high-quality information services and for location privacy. The proposed solution is based on the *imprecision concept*, which indicates the lack of specificity of location information (e.g., a user located in Milan is said to be in Italy). The authors propose to degrade location information quality and to provide obfuscation features by adding n points, at the same probability, to the real user position. The algorithm assumes a graph-based representation of the environment. When a user accesses a service asking for proximity information (e.g., asking for the closest restaurant), her location is perturbed by releasing a set O of points containing the real user position. The service receiving the request calculates the query result that is returned to the user: in the best case the user receives a single response, in other cases, depending also on the degree of obfuscation, it could receive a set of closest points of interest. Duckham and Kulik [37] present some obfuscation methods that are validated and evaluated through a set of simulations. The results show that obfuscation can provide at the same time both high quality of service and high privacy level.

Other proposals are based on the definition of a gateway that mediates between location providers and location-based applications. Openwave [38], for example, includes a location gateway that obtains users location information from multiple sources and delivers it, possibly modified according to privacy requirements, to other parties. Openwave assumes that users specify their privacy preferences in terms of a minimum distance representing the maximum accuracy they are willing to provide. Bellavista et al. [39] present a solution based on a middleware that balances the level of privacy requested by users and the needs of service precision. The location information is then provided at a proper level of granularity depending on privacy/efficiency requirements negotiated by the parties. Hence, downscaled location information (with lower precision and lower geographical granularity) is returned instead of exact user positions. This solution only considers a context based on points of interest, and it relies on the adoption of symbolic location granularity (e.g., city, country, and so on), forcing the privacy level to the predefined choices.

In summary, although obfuscation-based techniques are compatible with users specifying their privacy preferences in a common and intuitive manner (i.e., as a *minimum distance*), they present several common drawbacks. First, they do not provide a quantitative estimation of the provided privacy level, making them difficult to integrate into a full-fledged, location-based application scenario [22]. Second, they implement a single obfuscation technique according to which obfuscation is obtained by scaling (i.e., enlarging) the location area. An issue that is often neglected by traditional location obfuscation solutions is the possibility of defining and composing different obfuscation techniques to increase their robustness with respect

to possible de-obfuscation attempts performed by adversaries. Finally, they are meaningful in a specific application context only. With respect to the minimum distance specification, the value, "100 meters" is only meaningful when it is a good trade-off between ensuring a sufficient level of privacy to the user and allowing location-based applications to provide their services effectively. For instance, the value "100 meters" could be well suited to applications that provide touristic or commercial information to a user walking in a city center. By contrast, applications working in smaller contexts (e.g., inside an industrial department) are likely to require granularities much finer than 100 meters. Also, 100 meters can be largely insufficient for preserving user privacy in highly sensitive contexts.

15.4.3 Policy-Based Techniques

Another research field aimed at protecting location privacy is based on the definition of *privacy policies*. Privacy policies define restrictions that must be followed when the locations of users are used by or released to third parties.

Hauser and Kabatnik [40] address the location privacy problem in a privacy-aware architecture for a global location service, which allows users to define rules that will be evaluated to regulate access to location information. By means of these rules, a user can define the entities allowed to access her location data at a specified granularity level. The Internet Engineering Task Force (IETF) Geopriv working group [41] addresses privacy and security issues related to the disclosure of location information over the Internet. The main goal is to define an environment (i.e., an architecture, protocols, and policies) supporting both location information and policy data. Geopriv defines the Presence Information Data Format Location Object (PIDF-LO) [42] as an extension of the XML-based PIDF that provides presence information about a person (e.g., if a user is online or offline, busy or idle, away from communication devices or nearby). PIDF-LO is used to carry a *location object*, that is, location information associated with the privacy policies within PIDF. The Geopriv infrastructure relies on both *authorization policies* and *privacy rules*. Authorization policies pose restrictions on location management and access by defining conditions, actions, and transformations. In particular, a transformation specifies how the location information should be modified before its release, by customizing the location granularity (e.g., city neighborhood, country, and so on), or by defining the altitude, latitude, and longitude resolution. Privacy rules are instead associated with the location information and define restrictions on how the information can be managed. For instance, an authorization can state that a recipient is allowed to share a piece of location information that is associated with an expiration time.

Other works used the Platform for Privacy Preferences (P3P) [43] to encode users privacy preferences. P3P enables Web sites to define their privacy practices in an XML-based format, defining how data gathered from the counterparts will be managed (e.g., the purposes for which the information is collected, the retention time, and the third parties to whom the information will be released). A user then can check the privacy practices of the Web site she is visiting and, therefore, decide whether the data practices are compatible with her privacy preferences. Usually, the process of comparing user preferences and server practices is performed by agents. Although P3P is not intended to provide location privacy functionalities, it can be easily extended for this purpose. Hong et al. [44] provide an extension to P3P for representing user privacy preferences for context-aware applications. Langheinrich [45] proposes the *pawS* system that provides a privacy-enabling technology for end users. The pawS system allows data collectors, on the one side, to state and implement data-usage policies based on P3P, and, on the other side, to provide data owners with technical means to manage and check their personal information. Hengartner and Steenkiste [46] describe a method of using digital certificates combined with rule-based policies to protect location information.

In summary, policy-based techniques allow the definition of policies that simply can be adapted to the user's needs restricting the location management and disclosure. However, although the adoption of policies-based preferences is probably, from a privacy point of view, the most powerful and flexible technique, it can be very complex and unmanageable for end users. Often, users are not willing to directly manage complex policies and refuse participation in pervasive environments. Also, users remain unaware of the consequences of potential side effects in policy evaluation.

15.5 Conclusions and Discussion

Location privacy is a challenging research topic that involves both technological, legislative, and sociological issues. This chapter has described the technological context in which location privacy is increasingly becoming an important issue and whose management is critical for the diffusion of location-based services. Also, the chapter has presented the main techniques aimed at protecting location privacy in different contexts.

Several open issues still remain unsolved. A first requirement to be fulfilled in the near future is to find a privacy solution able to balance the need of privacy protection required by users and the need of accuracy required by service providers. Location privacy techniques, which are focused on users' needs, could make the service provisioning impossible in practice due to the excessively degradation of location measurement accuracy. A possible direction to avoid excessive degradation is the definition

of an estimator of the accuracy of location information (abstracting from any physical attribute of sensing technology) that permits to quantitatively evaluate both the degree of privacy introduced into a location measurement and the location accuracy requested by a service provider. Both quality of online services and location privacy could then be adjusted, negotiated, or specified as contractual terms. A first solution to the definition of a formal estimator of location accuracy, in the context of obfuscation-based techniques, has been provided in [47,48]. The estimator, named *relevance*, is validated in the context of a privacy-aware location-based access control (LBAC) [22] that provides access control functionality based on user location information.

A second issue that calls for consideration is the dynamicity of location information that often is erroneously considered and treated as static information. However, location information changes over time and can be exploited to infer sensitive information of the users. The definition of solutions able to reduce the amount of inference provided by location information is a subject of growing research efforts [9].

A third aspect that needs to be considered is the development of techniques to determine and counteract possible attacks aimed at reversing location privacy techniques and retrieving original sensitive information. In fact, if an attacker can reduce the effects of location privacy techniques, the privacy guaranteed to the users is reduced. For instance, in location path anonymization, trajectories of users enable an attacker to follow users' footsteps by exploiting the high spatial correlation between subsequent location samples. *Multi-target tracking* (MTT) algorithms [49] are used to link subsequent location samples to users who periodically report anonymized location information. By contrast, location obfuscation by scaling the location area can be simply bypassed by reducing the area of a reasonable percentage depending on the context.

To conclude, location information represents an important resource that can be used in different environments and whose usage could offer huge benefits to online services. However, the possible indiscriminated disclosure of location information can evoke a scenario in which location data are abused. We can expect that future research will integrate existing location privacy techniques to provide a more flexible and powerful solution.

Acknowledgments

This work was supported in part by the European Union under contract IST-2002-507591, by the Italian Ministry of Research Fund for Basic Research (FIRB) under project RBNE05FKZ2, and by the Italian MIUR under project 2006099978.

References

[1] Varshney, U., Location management for mobile commerce applications in wireless internet environment. *ACM Transactions on Internet Technology*, 3(3): 236–255, August 2003.

[2] Barkhuus, L. and Dey, A., Location-based services for mobile telephony: A study of user's privacy concerns. In *Proc. of the 9th IFIP TC13 International Conference on Human-Computer Interaction (INTERACT 2003)*, pp. 709–712, Zurich, Switzerland, September 2003.

[3] D'Roza, T. and Bilchev, G., An overview of location-based services. *BT Technology Journal*, 21(1): 20–27, January 2003.

[4] Privacy Rights Clearinghouse/UCAN. *A Chronology of Data Breaches*, 2006. http://www.privacyrights.org/ar/ChronDataBreaches.htm

[5] *Chicago Tribune*, "Rental Firm Uses GPS in Speeding Fine" Associated Press: Chicago, Tribune, July 2, 2001, p. 9.

[6] Lee, J-W., *Location-tracing sparks privacy concerns*. Korea Times. http://times.hankooki.com, 16 November 2004. Accessed 22 December 2006.

[7] Colbert, M., A diary study of rendezvousing: Implications for position-aware computing and communications for the general public. In *Proc. of the International 2001 ACM SIGGROUP Conference on Supporting groupwork*, pp. 15–23, Boulder, CO, September–October, 2001.

[8] Beresford, A.R. and Stajano, F., Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1): 46–55, 2003.

[9] Bettini, C., Wang, X.S., and Jajodia, S., Protecting privacy against location-based personal identification. In Jonker, W. and Petkovic, M., Eds., *Proc. of the 2nd VLDB Workshop on Secure Data Management*, pp. 185–199, LNCS 3674, Springer-Verlag, Heidelberg, Germany, 2005.

[10] Gedik, B. and Liu, L., Location privacy in mobile systems: A personalized anonymization model. In *Proc. of the 25th International Conference on Distributed Computing Systems (IEEE ICDCS 2005)*, pp. 620–629, Columbus, OH, June 2005.

[11] Gruteser, M. and Grunwald, D., Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of the First ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys 2003)*, San Francisco, CA, May 2003.

[12] Hong, J.I. and Landay, J.A., An architecture for privacy-sensitive ubiquitous computing. In *Proc. of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys 2004)*, pp. 177–189, Boston, MA, June 2004.

[13] Langheinrich, M., Privacy by design-principles of privacy-aware ubiquitous systems. In *Ubicomp 2001, Ubiquitous Computing, vol. 2201 of Lecture Notes in Computer Science*, pp. 273–291, Springer, Heidelberg, Germany, 2001.

[14] Duckham, M. and Kulik, L., A formal model of obfuscation and negotiation for location privacy. In Gellersen, H-W., Want, R., and Schmidt, A., Eds., *Proc. of the Third International Conference PERVASIVE 2005*, Munich, Germany, May 2005.

[15] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati. *Security in Decentralized Data Management*, Chap. K-Anonymity. Springer, Heidelberg, Germany, 2007.

[16] Samarati, P., Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6): 1010–1027, 2001.

[17] Getting, I., The global positioning system. *IEEE Spectrum*, 30(12): 36–47, December 1993.

[18] Parkinson, B. et al., *Global Positioning System: Theory and Application, vol. II*, Progress in Austronautics and Aerounautics Series, V-164. American Institute of Astronautics and Aeronautics (AIAA), Reston, VA, 1996.

[19] Gustafsson, F. and Gunnarsson, F., Mobile positioning using wireless networks: Possibilities and fundamental limitations based on available wireless network measurements. *IEEE Signal Processing Magazine*, pp. 41–53, July 2005.

[20] Sun, G. et al., Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs. *IEEE Signal Processing Magazine*, pp. 12–23, July 2005.

[21] Hengartner, U., *Enhancing user privacy in location-based services*. Technical Report CACR 2006–27, Centre for Applied Cryptographic Research, 2006.

[22] Ardagna, C.A. et al., Supporting location-based conditions in access control policies. In Lin, F-C., Lee, D-T., Lin, B-S, Shieh, S., and Jajodia, S., Eds., *Proc. of the ACM Symposium on Information, Computer and Communications Security (ASIACCS'06)*, pp. 212–222, Taipei, Taiwan, March 2006.

[23] *Teen Arrive Alive*. http://www.teenarrivealive.com

[24] *uLocate*. http://www.ulocate.com

[25] *CellSpotting.com*. http://www.cellspotting.com

[26] *Mologogo*. http://mologogo.com

[27] Cheverst, K. et al., Experiences of developing and deploying a context-aware tourist guide: The guide project. In *Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM-00)*, pp. 20–31, Boston, MA, August 2000.

[28] Marmasse, N. and Schmandt, C., Safe and sound a wireless leash. In Cockton, G. and Korhonen, P., Eds., *Proc. of ACM Conference on Human Factors in Computing Systems (CHI 2003)*, pp. 726–727, Ft. Lauderdale, FL, April 2003.

[29] *Enhanced 911—Wireless Services*. http://www.fcc.gov/911/enhanced/

[30] General Assembly of the United Nations. "Universal Declaration of Human Rights." United Nations Resolution 217 A (III). December 1948.

[31] Duckham, M. and Kulik, L., *Location privacy and location-aware computing*. In Drummond, J., Billen, R., and Joao, E., Eds., *Dynamic and Mobile GIS: Investigating Change in Space and Time*, Taylor & Francis, Boca Raton, FL, 2007.

[32] Beresford, A.R. and Stajano, F., Mix zones: User privacy in location-aware services. In *Proc. of the 2nd IEEE Annual Conf. on Pervasive Computing and Communications Workshops (PERCOM 2004)*, pp. 127–131, Orlando, FL, March 2004.

[33] Shannon, C.E., A mathematical theory of communication. *Bell System Technical Journal*, 27(379–423): 623–656, July, October 1948.

[34] Gruteser, M., Bredin, J., and Grunwald, D., Path privacy in location-aware computing. In *Proc. of the Second International Conference on Mobile Systems, Application and Services (MobiSys2004)*, Boston, MA, June 2004.

[35] Gruteser, M. and Liu, X., Protecting privacy in continuous location-tracking applications. *IEEE Security & Privacy Magazine*, 2(2): 28–34, March–April 2004.

[36] Ho, B. and Gruteser, M., Protecting location privacy through path confusion. In *Proc. of the IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Athens, Greece, 2005.

[37] Duckham, M. and Kulik, L., Simulation of obfuscation and negotiation for location privacy. In Cohn, A.G. and Mark, D.M., Eds., *Proc. of the COSIT 2005*, pp. 31–48, Ellicottville, NY, September 2005.

[38] Openwave. *Openwave Location Manager*, 2006. http://www.openwave.com/

[39] Bellavista, P., Corradi, A., and Giannelli, C., Efficiently managing location information with privacy requirements in wi-fi networks: A middleware approach. In *Proc. of the International Symposium on Wireless Communication Systems (ISWCS'05)*, pp. 1–8, Siena, Italy, September 2005.

[40] Hauser, C., and Kabatnik, M., Towards privacy support in a global location service. In *Proc. of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001)*, Paris, France, 2001.

[41] Geographic Location/Privacy (geopriv). September 2006. http://www.ietf.org/html.charters/geopriv-charter.html

[42] Peterson, J., *A Presence-based GEOPRIV Location Object Format*, December 2005. Request for comments (RFC) 4119. http://www.RFC-editor.org/rfc/rfc4119.txt.

[43] W3C. *Platform for privacy preferences (p3p) project*, April 2002. http://www.w3.org/TR/P3P/

[44] Hong, D., Yuan, M., and Shen, V.Y., Dynamic privacy management: A plug-in service for the middleware in pervasive computing. In Tscheligi, M., Bernhaupt, R., and Mihalic, K., Eds., *Proc. of the 7th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI'05)*, pp. 1–8, Salzburg, Austria, September 2005.

[45] Langheinrich, M., A privacy awareness system for ubiquitous computing environments. In Borriello, G. and Holmquist, L.E., Eds., *Proc. of the 4th International Conference on Ubiquitous Computing (Ubicomp 2002)*, pp. 237–245, Göteborg, Sweden, September 2002.

[46] Hengartner, U. and Steenkiste, P., Protecting access to people location information. In Hutter, D., Müller, G., Stephan, W., and Ullmann, M., Eds., *Proc. of First International Conference on Security in Pervasive Computing*, pp. 25–38, Boppard, Germany, March 2003.

[47] Ardagna, C.A. et al., A middleware architecture for integrating privacy preferences and location accuracy. In *Proc. of 22nd IFIP TC 11 International*

Information Security Conference (IFIP SEC2007), Sandton, Gauteng, South Africa, May 2007.

[48] Ardagna, C.A. et al., Managing Privacy in LBAC Systems. In *Proc. of the Second IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC-07)*, Niagara Falls, Ontario, Canada, May 2007.

[49] Reid, D.B., An algorithm for tracking multiple targets. *IEEE Transactions on Automatic Control*, 24(6): 843–854, December 1979.