Implicit Authorization for Social Location Disclosure

Georg Treu[1], Florian Fuchs[1], and Christiane Dargatz[2]
[1]Mobile and Distributed Systems Group, Institute for Informatics
[2]Department of Statistics
Ludwig-Maximilian University Munich, Germany
[georg.treu|florian.fuchs]@ifi.lmu.de, christiane.dargatz@stat.uni-muenchen.de

***Abstract*— Being increasingly equipped with highly-accurate positioning technologies, today's mobile phones enable their owners to transmit their current position over the cellular network and share it with others. So-called location-based community services make use of this possibility, for example for locating friends, co-workers or family members. Of course, these services give target persons control about the way location data may be accessed by others. So far, this is done by the target explicitly granting or denying permissions through authorization policies or ad-hoc authorization. Unfortunately, apart from bringing along high management effort, the concept of explicit authorization in such a privacy-sensitive application entails the disadvantage of social difficulties.**

In this paper we introduce the concept of implicit authorization, which has reciprocity as its central element: Another person is granted access to a certain target's location information implicitly by the target accessing the information of that other person as well. The technique aims to reduce social pressure on the target person when deciding whether a certain person may locate her or not. Also, the target person is relieved from management overhead. Several realizations of implicit authorization are proposed. They differ in the service pattern (reactive/proactive) they are useful for and the way a once given access grant is revoked.

***Index Terms*— community LBS, proactive LBS, social disclosure, authorization, reciprocity, ambiguity**

I. MOTIVATION

With the mass market introduction of cellular phones in the early 1990s, the paradigm of always being available changed the way we think and act. In recent time, mobile phones are increasingly equipped with highly-accurate positioning technologies like GPS, which not only facilitates local applications like navigation, but also allows individuals to transmit their current position over the cellular network and share it with others. Suddenly, it becomes easily possible that everybody can always be located by anybody.

So-called *location-based community services (LBCSs)* make use of this technique. Examples are friend finder services [1] [2], child trackers, dating services, and location-enhanced instant messaging (IM) services [3].

This paper is based on "Implicit Authorization for Accessing Location Data in a Social Context" by G. Treu, F. Fuchs, and C. Dargatz, which appeared in the Proceedings of The Second International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, April 2007. © 2007 IEEE.

According to the classification in [4], an LBCS can be either *reactive* or *proactive*. In the former case the location information of the target is presented to the user only when the user explicitly asks for it. An example is a simple friend finder application which has a button for the user that allows him to locate one or more of his friends and show their position on a map. In the latter case location information is automatically displayed to the user on the arrival of a certain pre-defined spatial condition, defined in terms of the position(s) of the target(s). An example is an office tracker application which automatically notifies the co-workers of the target person as soon as she has approached the work place below a certain distance.

In order to be acceptable at the market, LBCSs give target persons control about the way location data may be accessed. So far, this is done by *explicit access authorization*, which requires an explicit yes or no decision by the target whether a given user may access her location data or not and which can be implemented in two general ways. First, the target can deposit *authorization policies* with the LBCS provider, which exclude or include certain individuals from accessing her location information. The second strategy is *ad-hoc authorization*, where the target person is asked for approval each time her location data is to be transferred to the user.

Unfortunately, explicit authorization has several disadvantages. First, it is associated with considerable management effort for the user, which in one case is dedicated to the a-priori definition of policies and in the second case to the target's manual interaction with the service. Second, explicit authorization has a high potential of introducing social difficulties. For instance, a user who wants to inquire the location of a target person may feel rejected by the target if access is not granted. On the other hand, the target may feel socially pressured to grant the inquirer access in order to avoid possible negative social implications.

For circumventing these problems, this paper introduces the concept of *implicit authorization*. An inquirer A is granted access to the location information of target B, only if B in turn has previously attempted to access the location information of A. That is, by accessing the location information of another person, that person is implicitly granted access to one's own location.

We believe the technique is better socially acceptable than explicit authorization for the following two reasons. First, *reciprocal information exchange* is enforced, which is generally desirable for privacy-sensitive applications like LBCS. Second, *plausible deniability* is built in by the mechanism as explicit denial decisions by the target are simply disabled. Instead, the concept provides *ambiguity* and thus ”makes space for stories” [5], because denied access attempts can be attributed to the target having not localized the other person, which in turn can have multiple causes, e.g. economical ones.

Different realizations of implicit authorization are presented, which differ in the service pattern (reactive/proactive) they are useful for and the way a once given access grant is revoked. One revocation technique is based on leases: After a certain amount of time an access right ceases automatically. If a renewal is desired, the target needs to locate the user again. Another proposed technique uses a whitelist of limited size for revoking access rights: If a new user is added to the whitelist and if the maximum size of the list is reached, then the user in the list which was least recently localized by the target loses his access grant automatically.

The paper is structured as follows: Section II identifies basic requirements on an authorization scheme for LBCSs, such as usage simplicity and control. Furthermore, two general concepts that enhance social acceptability are presented, which are reciprocity and ambiguity. Section III reviews existing techniques of explicit authorization. Section IV introduces the novel concept of implicit authorization and discusses the three given realizations. The work is concluded in Section V.

II. Challenges

We consider the following requirements on an authorization mechanism for LBCSs as the most essential ones.

A. Control

The mechanism should give the target control about who may access her location information at any time. That is, decisions made by the mechanism concerning denial or approval of access should reflect the current attitudes of the target as well as possible.

For expressing this quality in a more formal way, we introduce the terms *correctness* and *completeness* of authorization, which are defined in analogy to the metrics *precision* and *recall* common in *information retrieval (IR)*. For a given time span, correctness denotes the fraction of those location disclosures approved by the mechanism which were also desired by the target. Completeness, in turn, denotes the fraction of those location disclosures desired by the target to be approved which were actually approved by the mechanism. Mathematically, correctness and completeness are defined in close analogy to precision and recall, whereby instead of *positives* and *negatives*, we speak of disclosure *approvals* and *denials*, respectively. Similarly to IR, the target’s agreement is reflected by qualifying a disclosure decision as *true* or *false*, respectively.

Also in analogy to precision and recall, achieving a high level of correctness without considering completeness, or vice versa, is fairly simple. Consider for instance an overly restrictive system which discloses location data to nobody. Obviously, that would yield excellent correctness as no *false approvals* can happen. The achieved completeness, however, would be poor as, potentially, there could be a lot of *false denials*. Another example is an overly permissive approach which discloses a target’s location to everybody. The result would be perfect completeness as no *false denials* can happen, but the correctness would be poor, because of the possibly high number of *false approvals*. To conclude, the challenge is to design an authorization mechanism which guarantees high values for correctness and completeness at the same time.

B. Simplicity

Despite giving the target the desired control, an authorization mechanism should be simple enough to be adopted in the first place.

Simplicity is naturally associated with good usability of the mechanism. Obviously, time and effort the target has to spend for managing an authorization mechanism should be reduced as far as possible. Such management effort can include the a-priori definition of authorization policies, or, in case of authorization on request, ad-hoc interaction with the authorization procedure. Of course, the mechanism should be intuitive to use and not too complex in order to be practicable for everyone who uses the service. The latter aspect represents a particular problem for authoring privacy policies [6], which need to be fine-tuned and reworked on a regular basis in order to reflect current target attitudes.

Simplicity is also desirable with regard to the effort to implement the mechanism and, possibly, integrate it with existing solutions, which is probably one of the most important considerations for LBCS providers. In this aspect, between the two introduced explicit authorization techniques, the policy-based approach seems to have clear advantages over ad-hoc authorization as it allows the definition of policies to be decoupled from their enforcement. This way, no dedicated user interface is needed for prompting the target for approval, which in turn enables an easier integration of more diverse terminal types and positioning methods like network-based ones, where a component located in the network derives the target’s current position without communicating with her mobile device. For a good overview about positioning technologies, see [7].

C. Social Acceptability

If LBCSs are really to become a part of people’s day to day life, their social implications should be profoundly analyzed and possible negative consequences should be avoided by design, a task that goes beyond classical requirements engineering. If one takes a look at recent

literature in that field, e.g. [8] [9], social issues of privacy are more and more emphasized. Two related concepts seem to be especially important, see also [3]: *reciprocity* and *ambiguity*.

1) Reciprocity.: This is a well-known principle for establishing balance between parties that engage in a privacy-sensitive exchange of information. The principle states that the amount of information transferred from person A to person B should be roughly the same as the information that is transferred from B to A. According to [10], who discuss the principle for context-aware services, reciprocity helps to avoid negative social situations. The authors compare these negative situations to economical inefficiencies which arise in a market environment when certain people take advantage of insider knowledge.

While related works so far promote reciprocity for achieving balance of mere information flows, a potential privacy risk still exists when the interest in receiving the information is not well-balanced. Suppose person A and person B are socially related. As A feels that B should be able to locate her, she authorizes B to do so, however, only under the premise that the flow of location information between the two is balanced (”classical” reciprocity). That is, whenever B requests the position of A, B also has to reveal his own position to A.

However, while being already advantageous over non-reciprocal sharing, a problem for A with this setup can still arise when A is actually not interested in knowing B's location, but B is in knowing A's. Imagine that B is rather indifferent about revealing his own location several times a day to A, if only B can determine A's position as often as desired. This could lead to A feeling controlled by B.

As a conclusion, we suggest that an authorization mechanism aimed to balance the privacy between persons should not only guarantee symmetric information flows, but also consider mutual interest in receiving the exchanged information.

2) Ambiguity.: Being marked by U.S. politics in the 1950s, the term *plausible deniability* originally refers to obscuring operations by the then newly-formed Central Intelligence Agency. In the meantime it has also become an essential concept for achieving personal privacy in pervasive systems [11]. Plausible deniability denotes that the potential observer of another person cannot determine whether a lack of disclosure was intentional or not. An obvious example is a person who does not want to be located and decides to turn off her mobile device. From the location inquirer's point of view, it is not clear whether the person being *temporarily unavailable* is deliberate or due to technical problems like missing radio contact.

Being strongly related to plausible deniability, *ambiguity* is discussed by [5] and [12] for *personal communication systems (PCSs)* like push-to-talk. When unsuccessful communication attempts are mediated to the caller in a way that can be ambiguously interpreted, possible social difficulties arising between caller and called person in the aftermath are reduced, a process referred to as ”face work”. Apart from possible technical problems, space for ambiguous interpretation (”stories”) can be made, e.g. by attributing rejected calls to economical resources of the called person, which would have been consumed by taking the call. Based on sociological studies it is stated that, in order to enable ”face work”, the ”story” presented to the caller needs not be extremely convincing. More important is that ambiguous interpretation is possible, so that both persons can save face. Ambiguity is less focused than plausible deniability on mediating an explicit denial decision to the observer and thus fits well with the implicit authorization technique proposed later.

Applied to LBCSs, ambiguity avoids directly repulsing a location inquirer, which in turn reduces the social pressure on the target person when deciding about who may locate her and who not. With ambiguity it remains unclear to the inquirer whether a denied location disclosure was deliberate by the target person, or if other causes, e.g. limited economical resources, have kept the target from disclosing her location. Especially because computer systems are getting more and more reliable, possible technological causes for refused disclosures, which represent the ”classical” way of ambiguity, are diminishing. Therefore, new ways to support ambiguity in LBCSs and context-aware services need to be discovered, which is one of the main objectives of this paper.

III. Existing Authorization Techniques

This section reviews existing techniques of explicit authorization – policy-based, ad-hoc, and hybrid authorization – in more detail.

A. Policy-based.

According to [13], an authorization policy is an assertion that a certain amount of information may be released to a certain entity under a certain set of *constraints*. A policy typically consists of various types of constraints, see also [14]: *Actor constraints* restrict access to a limited set of inquirers, *time constraints* to publishing location data only at certain times, and *location constraints* limit access to certain predefined locations. By specifying *accuracy constraints*, a target can intentionally degrade the accuracy of emitted location information. Accuracy constraints have also been proposed as an extension to Geopriv [15], a well-known protocol standard for privacy-aware exchange of location data. Authorization policies are typically defined by the target but enforced by a different actor on behalf of the target, e.g. the LBCS provider.

B. Ad-hoc.

While policies are deposited in advance, ad-hoc authorization interactively involves the target in the authorization procedure. Ad-hoc authorization is promoted by work originated from the Place Lab project [16]. Examples are Reno and Boise, both being systems for social location disclosure based on numerous practical evaluations and

user studies, compare [17] [18] [19]. For increasing the social acceptability of ad-hoc authorization, several techniques are proposed. One is using *silent time-outs*, that is, if the target does not respond to an authorization request for a given time-out interval, the inquirer is automatically denied access and the request is discarded. This way, room for ambiguity is created, because it is not clear to the inquirer whether the target has deliberately refused the request or not. Furthermore, ad-hoc authorization enables fine-grained deception techniques, which are useful when the target person decides to publish a false location to the inquirer, e.g., to avoid certain situations of social pressure. Also, with ad-hoc authorization the target can better examine the reason of the inquirer's request, which generally enhances reciprocal exchange of information. Note that ad-hoc authorization is suited rather for reactive than for proactive LBCSs. The latter should trigger events automatically, which is somewhat contradictory to the concept of manual (ad-hoc) interaction.

C. Hybrid.

Authorization by policy and ad-hoc authorization can also be combined. By so-called *notification constraints*, which may be part of an authorization policy or not, a target can define certain situations in which she wishes to be prompted for ad-hoc approval. Many mobile network operators, when externally requested to locate a subscriber's mobile terminal, rely on that combination. *Notice*, that is, a target is generally informed about attempts of locating her, can also happen in a purely passive way. It is seen as a fundamental technique for privacy improvement, see also [20].

Noteworthy is an investigation by [21], saying that a target's attitude toward authorizing an inquirer is influenced stronger by the inquirer's identity than by the current situation of the target. That is, a once taken authorization decision regarding a given person may stay relatively constant for different situations.

D. Conclusion.

While explicit authorization gives the target control about her location data, it also brings up two inevitable problems. First, despite certain techniques for reducing social impact (silent time-outs, selective deceiving, etc.), a potential inquirer has good reason to assume denial decisions are made in an explicit way, which strongly limits space for ambiguity. Second, extra time and effort of the target is needed for managing the mechanism, which is typically the higher the more fine-grained the desired control is. A related and complex issue is the provisioning of an appropriate user interface for the target person.

As a possible solution, the next section presents the novel approach of implicit authorization.

IV. Implicit Authorization

This section defines and discusses implicit authorization as a generally new paradigm for granting other persons access to one's own location information. Concrete realizations for both reactive and proactive LBCSs illustrate the paradigm.

Implicit authorization has reciprocity as a central element: Location disclosure to a certain person A is implicitly admitted by a certain target person B when B requests a location disclosure from A as well. The scheme is suited for LBCSs where members of a community voluntarily exchange location information among themselves and were the information exchange is per se rather balanced. One example is a typical friend finder service. Another is an LBCS which allows co-workers to locate each other for coordination purposes. The mechanism is not suited for LBCSs that rely on single-sided tracking, like a child tracker or a system used for elder care. However, in these latter applications the need for reducing social pressure also seems less prevalent.

The technique applies to proactive as well as to reactive LBCSs. Proactive LBCSs, which are not request-based but triggered by spatial events, have a natural ambiguity feature built in: The ambiguity lies in the fact that, if the user does not receive any notification for a certain event with respect to the target she has subscribed to, it can have two reasons. First, the target may have blocked the disclosure. Second, the event simply has not occurred.

However, while being an advantage in general, this natural ambiguity can only be carried to a certain level. In the introductory example, where co-workers are to be informed as soon as the target enters the work place, they can tell by physical observation whether the event in fact happened or not. Hence, additional ambiguity is also needed for proactive LBCSs. Reactive LBCSs do not exhibit this built-in ambiguity, because when requesting the location of the target person, the user explicitly waits for a result message.

In order to account for the different properties of reactive and proactive LBCSs, the following first discusses two versions of implicit authorization for reactive LBCSs. Then, a version suited for proactive LBCSs is presented.

A. Implicit Authorization for Reactive LBCSs

Implicit authorization for reactive LBCSs means that the request of user A for the location of user B will only be answered positively if B has requested the location of A before. That is, by showing interest in somebody else's location (that is, by requesting the location), one implicitly grants the person access to one's own location.

Obviously, inquiring another person's location requires a certain effort, e.g. time or monetary costs spent for mobile bearer services or other limited resources. Hence, in case a person is not granted access, it is easier for the target person to argue that certain resource constraints have kept her from locating the person, which would have granted the access for that person. Thus, in contrast to explicit authorization, the mechanism provides a richer resource for ambiguity, which reduces social pressure. Also, apart from providing reciprocal information flows,

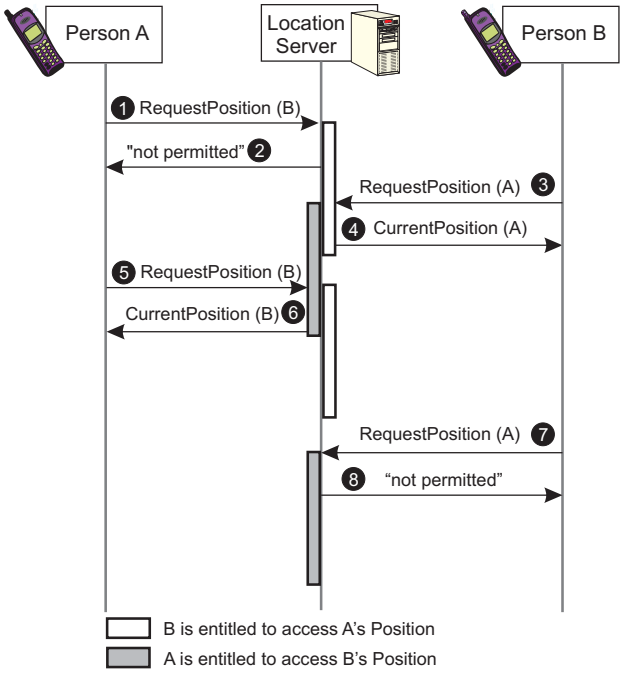

Figure 1. Implicit Authorization for Reactive LBCSs with Revocation based on Leases.

mutual interest in the exchanged information is enforced as postulated in Section II-C.1.

The mechanism is simple to use and provides control for the target, who can decide before locating another person whether she wants to sacrifice some of her own privacy in turn. By deliberately avoiding to locate certain persons, a high value for correctness can be achieved. At the same time a high value for completeness is possible, as every user in the system is free to try to locate each other. User identifiers in the system can be static and publicly known, like email addresses. No additional management effort and no user interface dedicated to authorization is needed, because permission management is handled implicitly, simply through using an LBCS.

A possible source of irritation is that first-time locating attempts are always unsuccessful, although the target might be willing to disclose. However, as users are aware of the mechanism, they can handle this situation, e.g. by initially encouraging the target to locate them once.

A bigger problem, we think, is finding an easy-to-understand and practicable method for revoking once-granted access permissions. Therefore, the following discusses two different revocation methods, one using time-based leases, one using whitelists of limited size.

1) Revocation Based on Leases: In this version of implicit authorization, access is revoked based on so-called *leases* whose validity is limited in time or another dimension (see below). A lease is associated with exactly one target-inquirer relation. It can be extended only by the target re-locating the inquirer. Consider Figure 1 as an illustration. Each time the location server receives a request, it uses a simple rule for deciding on the disclosure of the requested information: The request of user A for the location of user B will only be answered positively if B has requested the location of A less than a particular time period ago. A's first attempt to locate B is rejected (1 and 2), because B has not inquired A's position yet. However, due to the request a lease allowing B to locate A is deposited at the server. B makes use of the lease soon (3 and 4), which in turn entitles A to locate B some time afterward (5 and 6). After A not locating B for a longer period of time, B's lease times out and her positioning attempt is rejected (7 and 8).

In addition to being limited by a time frame, the validity of the lease can be linked with different conditions and combinations of these, e.g.:

- A lease can be valid for a certain *number of requests*. That is, it authorizes the lease holder to access the location of the lease granter n times.
- A lease can be valid for a certain *spatial region*. That is, it authorizes the lease holder to access the location of the lease granter only when the lease granter is located within a certain range from where the lease was created.

In order to learn more about the long-term behavior of the mechanism, the following evaluations are carried out.

We investigate the practicability of our approach in the case that two participants actually *want* to authorize each other and thus request each other's location according to a given probability distribution. This is done using simulations on a statistical model. Here, we summarize our findings and refer to [22] for details.

a) Model and Scenarios: We assume two participants who access each other's location. The number of accesses per hour for each participant i is modeled by a Poisson distribution with rate parameter λ_i. We assume that all accesses are legitimate and should therefore be granted. When participant i accesses the location of participant j, our proposed authorization system automatically grants j access to i's location for the following δ_i hours (denoted as *lease time*). With no real data at hand, the value ranges for λ_i and δ_i were chosen based on common sense.

We investigate two scenarios: In *scenario 1:1*, both participants exhibit the same access rate, while in *scenario 3:1*, participant one has an access rate three times higher than participant two. Applied to a friend-finder service, scenario one simulates two friends with totally balanced interest in locating each other, while scenario two corresponds to a less balanced relation, where one person is more interested in locating another one than the other way round.

b) Effect of Access Rate: The first experiment investigates the dependence between access rate and the proportion of granted accesses assuming a fixed lease time of 48 hours.

In scenario 1:1, the access rate for each participant varies from once a week to 6 times per day. Figure 2 shows the simulation results for the total number of accesses: In order to achieve an approval rate of at least 95%, at least 3.2 accesses per day are required in total.

This translated to about 1.6 accesses per day for each participant.

In scenario 3:1, the access rate for participant one varies from 1.5 per week to 9 per day, while participant two has access rates from 0.5 per week to 3 per day. Here, the effect is of course different for each participant (see Figure 2). In order to achieve an approval rate of at least 95% for both participants, access rates of at least 6.5 requests per day for participant one and at least 1.6 requests per day for participant two are required.

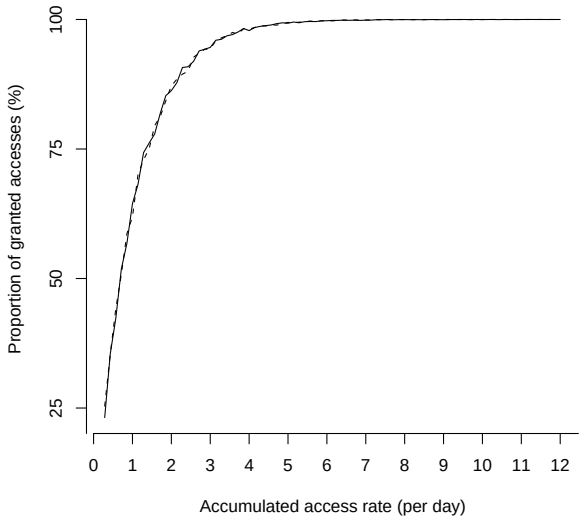

Figure 2. Two participants with identical access rates and a lease time of 48h

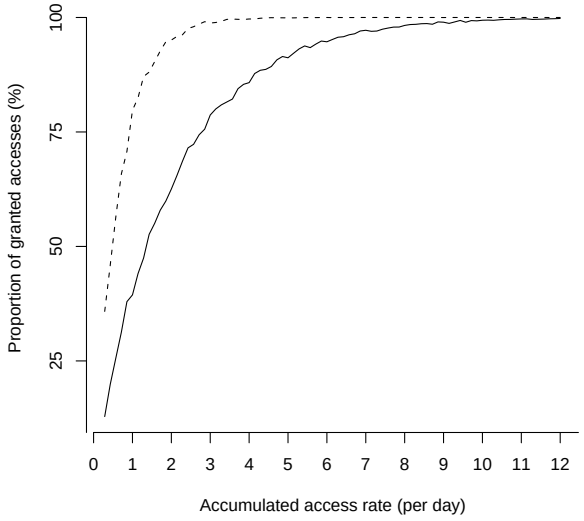

Figure 3. Two participants with access rate ratio of 3:1 and a lease time of 48h

c) Effect of Lease Time: In a second experiment, we investigate the effect of lease time length on the proportion of granted accesses. Here, access rates for both participants are assumed as 3 per day in scenario 1:1 and 4.5 and 1.5 per day in scenario 3:1. Lease time length varies from one hour to three days.

In scenario 1:1, a lease time of at least 24 hours is required in order to achieve at least 95% of correctly granted accesses. In scenario 3:1, participant one requires a lease time of at least 49 hours for achieving at least 95% of granted accesses. Participant two, being queried more frequently, requires a minimum lease time of 16 hours.

d) Summary: The mechanism is quite reliable in case two persons locate each other relatively often and if the interest in each other's location is balanced. Otherwise, denied access attempts get more frequent, at least regarding the person that is requested more seldom by the other. Thus, applications for single-sided tracking, like child- or pet-finders, or ones used only seldom, like emergency services, are probably not compatible with lease-based revocation. However, the mechanism seems to be well suited when balance of interest is actually desired and when the LBCS is used more frequently, as conceivable for typical friend finder services. The selection of the ideal lease time is a trade-off: Long periods increase reliability, while shorter ones increase control in terms of correctness and also enhance ambiguity in case a target decides not to renew a lease. For the assumed access rates, lease times between 24h and 48h seem most appropriate.

2) Revocation Based on Whitelists: The previously described revocation scheme is very sensitive to changes in usage patterns of the LBCS: The lease time is selected for a particular frequency of service usage. If either of the two involved parties diverge from the assumed frequency, revocation based on temporary leases will produce false denials.

As an improvement for scenarios with volatile usage frequencies, we propose a different revocation scheme that uses FIFO whitelists. Like before, users deposit their location information at a central location server and request the location information of others from it. However, this time a different rule is used for deciding on the disclosure of this information: The request of user A for the location of user B will only be answered positively if B is one of the n most recent users who requested the location of A. So at any point in time, maximum n users are granted access to the location of user A. This is why we speak of a whitelist for user A with n entries. The list is updated every time user A requests the location of somebody else. When A requests the location of C, C is added to the head of the list and the user who was previously at position n is removed from the list. The whitelist therefore exhibits a FIFO (first in, first out) behavior. Figure 4 illustrates the procedure for $n = 3$.

This scheme has the following advantages: It enforces reciprocal exchange of location information without imposing temporal restrictions in contrast to the previous schemes. The scheme is independent from usage

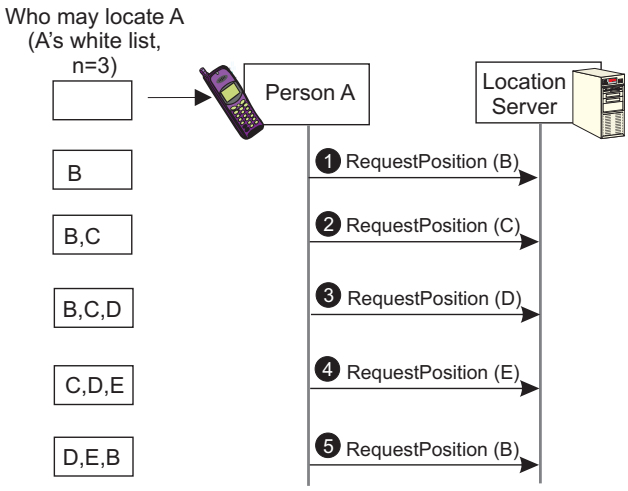

Figure 4. Implicit Authorization for Reactive LBCSs with Revocation based on Whitelists.

frequency and therefore more robust in scenarios with volatile usage frequencies.

At the same time, the number of possible disclosure relationships is limited, which could be seen as a disadvantage. However, this also allows the owner of the whitelist to control location disclosure to a good degree. E.g., by locating random persons who certainly will not locate back, such as celebrities, the target can remove any unwanted inquirer from his list at once. This leads to a higher correctness than with leases in case the target suddenly changed his mind about a certain user. In addition, it provides the user with ambiguity as denied location requests can be justified as being due to other location requests that had to be carried out by the user in between (resulting in the removal of previous users from the whitelist).

An important decision is the choice of n. It should be small enough to result in continuous adaptation of the whitelist and at the same time large enough to enable stable disclosure relationships within a narrow circle. Regarding the fact that location information is very privacy-sensitive and that normally the circle of very close relationships of a person is rather small, $n = 5$ seems reasonable to us. However, user studies will be necessary for a better-founded selection. Also, n may depend on the type of LBCSs and/or the type of the target community and should be chosen accordingly. E.g., adults may be more averse toward location disclosure than teenagers, resulting in a smaller n for adults.

B. Implicit Authorization for Proactive LBCSs

The previously described schemes are designed for reactive LBCSs. Proactive LBCSs, however, have different characteristics, e.g. that at the time of service initiation, the concrete moment and the number of location disclosures is not yet known. Still, starting with the subscription to a target's location, there is the *possibility* of receiving his location information anytime. This "potential knowledge" should be balanced as well, e.g., by requiring the *potential* disclosure of the inquirer's location information in return. Implicit authorization represents an attractive authorization scheme for this.

A subscription of person A to a particular event regarding person B entitles B to receive events regarding A as well. This way, a reciprocity of subscriptions is enforced, which takes account of the *possibility* of location disclosures. By unsubscribing from user B, user A will not receive any events related to user B anymore. At the same time, user B will not receive any events related to user A even if user B is still subscribed to user A. Figure 5 illustrates the technique. A subscribes to event $Ev1$ regarding B (1). Soon afterward, A triggers the event herself (2). However, since B is not subscribed yet, the event is not forwarded. At step (3) B also subscribes to the event from A, which finally entitles A to receive notifications of this event type from B. Hence, when in step (4) B triggers the event, it is forwarded to A (5). After that, A unsubscribes from the event (6) which at once revokes B's grant to receive the next event from A (7). Finally, B also unsubscribes from A's events (8).

The application of implicit authorization to proactive LBCSs carries particular advantages: It enables the user to control disclosure of location information to other users. At the same time, there is no management overhead or specialized user interaction necessary, as disclosing information is implicitly coupled with requesting (future) information. Finally, ambiguity is enhanced as the absence of notifications can always be justified with the fact that interest is not mutual or that the overhead of receiving events regarding a certain person is just too big for the receiving person. This avoids the feeling of repulse for a person who waits in vain for location events of another.

In analogy to the whitelist-based revocation from above, a variation of this scheme is to limit the number of subscriptions a user can place. This way, an additional source of ambiguity is created: If user B happens to *know* (for example because user B and A came across each other) that an event related to user A should have been fired but was not fired, then B can argue that the number of subscriptions is limited and that it was necessary to subscribe to somebody else's location events in the meantime.

C. Discussion

One risk associated with implicit authorization is that the mechanism could be perceived as artificial chicanery and not be accepted. The target person might wonder why she cannot simply authorize an inquirer person without having to locate the person first. However, we believe that the technique has the potential of being regarded as a very economical way of exercising control – designed to avoid the management overhead associated with explicit authorization. Put into other terms, while our motivation for designing the mechanism was to reduce social pressure, one way to promote it to actual users is to emphasize its ease of use.

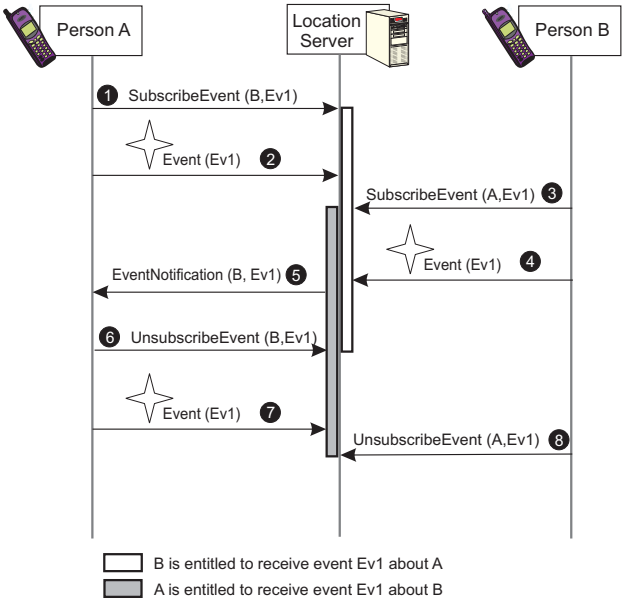

Figure 5. Implicit Authorization for Proactive LBCSs.

Another open issue is whether reciprocal location disclosure can always be assumed for LBCSs used by independent adults (excluding child trackers and elder care). This work simply did so. However, when single-sided tracking is actually desired, at least by one party (e.g., a boss wants to track her employee, while the employee does not want to track the boss), this mechanism is not useful. A related question which we cannot and do not want to answer is whether single-sided tracking is ethical or not and whether it should be promoted or not. We think that by giving the user a new tool at hand, such as implicit authorization, certain social norms, such as "Should single-sided tracking be supported or not?", at least have the chance to develop more freely, because it enables users to choose between different alternatives for authorization.

V. Conclusions and Future Work

The paper presented a novel paradigm for authorizing social disclosure of location data: *Implicit authorization* reduces management overhead and social pressure. Concrete realizations for reactive and proactive LBCSs were discussed, including versions with revocation based on leases and FIFO whitelists. It was analyzed why the techniques are particularly well-suited for different variations of equilateral LBCSs like friend finder services. They are simple to use, provide control, and feature reciprocity as well as ambiguity.

The proposed mechanisms are currently being tested within the device-centric LBS middleware framework TraX [4], which especially supports community services. Future work is also concerned with analyzing the legal implications of the mechanism, e.g. with respect to regulation efforts for personal data collection like [23]. Last but not least, implicit authorization is not specific for protecting location data. The principle may apply to further types of personal information users might want to share.

References

[1] "Dodgeball.com," 2006, http://www.dodgeball.com, last access 2006/09/08. [Online]. Available: http://www.dodgeball.com

[2] "Socialight," 2006, http://socialight.com, last access 2006/03/07. [Online]. Available: http://socialight.com

[3] M. Raento and A. Oulasvirta, "Privacy management for social awareness applications," in *Proc. of Workshop on Context Awareness for Proactive Systems (CAPS 2005)*, 2005.

[4] A. Küpper, G. Treu, and C. Linnhoff-Popien, "Trax: A device-centric middleware framework for location-based services," *IEEE Communications Magazine*, vol. 44, no. 9, September 2006.

[5] P. M. Aoki and A. Woodruff, "Making space for stories: ambiguity in the design of personal communication systems," in *Proc. of CHI '05*. New York, NY, USA: ACM Press, 2005, pp. 181–190.

[6] C.-M. Karat, J. Karat, C. Brodie, and J. Feng, "Evaluating interfaces for privacy policy rule authoring," in *Proc. of CHI '06*. New York, NY, USA: ACM Press, 2006, pp. 83–92.

[7] A. Küpper, *Location–based Services — Fundamentals and Operation*. John Wiley & Sons, Aug. 2005.

[8] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in *Proc. of Conference on Designing Interactive Systems (DIS '04)*. New York, NY, USA: ACM Press, 2004, pp. 91–100.

[9] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. D. Abowd, "Developing privacy guidelines for social location disclosure applications and services," in *SOUPS '05: Proc. of the 2005 symposium on Usable privacy and security*. New York, NY, USA: ACM Press, 2005, pp. 65–76.

[10] X. Jiang, J. I. Hong, and J. A. Landay, "Approximate information flows: Socially-based modeling of privacy in ubiquitous computing," in *Proc. of Ubicomp '02*. London, UK: Springer-Verlag, 2002, pp. 176–193.

[11] S. Lederer, I. Hong, K. Dey, and A. Landay, "Personal privacy through understanding and action: five pitfalls for designers," *Personal Ubiquitous Computing*, vol. 8, no. 6, pp. 440–454, 2004.

[12] K. Boehner and J. T. Hancock, "Advancing ambiguity," in *Proc. of CHI '06*. New York, NY, USA: ACM Press, 2006, pp. 103–106.

[13] J. Cuellar, "Location information privacy," in *Geographic Location in the Internet*, B. Sarikaya, Ed. Norwell, MA: Kluwer Academic Publishers, 2002, pp. 179–212.

[14] G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 56–64, 2003.

[15] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, and J. Polk, "A document format for expressing privacy preferences for location information. draft-ietf-geopriv-policy-08.txt," February 2006. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-geopriv-policy-08.txt

[16] A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, and al., "Placelab: Device positioning using radio beacons in the wild," in *Proc. of Pervasive 2005*, ser. LNCS. Munich, Germany: Springer-Verlag, May 2005, pp. 116–133.

[17] S. Consolvo, I. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations: why, when, & what people want to share," in *Proc. of CHI '05*. New York, NY, USA: ACM Press, 2005, pp. 81–90.

[18] I. Smith, S. Consolvo, A. LaMarca, J. Hightower, and al., "Social disclosure of place: From location technology to communications practices," in *Proc. of Pervasive 2005*, ser. LNCS. Springer-Verlag, May 2005.
[19] G. Iachello, I. Smith, S. Consolvo, G. D. Abowd, and al., "Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service," in *Proc. of Ubicomp 2005*, ser. LNCS. Springer-Verlag, September 2005, pp. 213–231.
[20] M. Langheinrich, "Privacy by design – principles of privacy-aware ubiquitous systems," in *Proc. of Ubicomp 2001*, ser. LNCS, G. Abowd, B. Brumitt, and S. Shafer, Eds., vol. 2201. Springer, 2001, pp. 273–291. [Online]. Available: http://citeseer.nj.nec.com/491722.html
[21] S. Lederer, J. Mankoff, and A. K. Dey, "Who wants to know what when? privacy preference determinants in ubiquitous computing," in *Proc. of CHI '03*. New York, NY, USA: ACM Press, 2003, pp. 724–725.
[22] G. Treu, F. Fuchs, and C. Dargatz, "Implicit authorization for accessing location data in a social context," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*. Los Alamitos, CA, USA: IEEE Computer Society, 2007, pp. 263–272.
[23] "Directive 2002/58/EC on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector," *Official Journal of the European Communities of 31 July 2002*, no. L 201/37, July 2002.

Georg Treu received his Ph.D. in Computer Science from the Ludwig-Maximilians-University Munich in 2007 and his Master's degree from the Technical University of Munich in 2004. His research interests include location-based services (LBSs), in particular, proactive multi-target LBSs, and mechanisms for location privacy.

Florian Fuchs received his Master's degree in Computer Science from the Technical University of Munich in 2005. He is currently a Ph.D. student at Siemens Corporate Technology and the Mobile and Distributed Systems Group, Ludwig-Maximilians-University Munich. His research interests include context-aware services and, in particular, context modeling and reasoning on context information.

Christiane Dargatz received an M.Sc. in Computational Modeling from Brunel University West London in 2003 and a Master's degree in Mathematics from the University of Hanover in 2005. She is currently a Ph.D. student at the Institute of Statistics, Ludwig-Maximilians-University Munich. Her research focuses on the stochastic analysis of interactions between individuals in diverse fields such as mobile services and epidemiology.