In: Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001), Paris, 2001

Towards Privacy Support in a Global Location Service

Christian Hauser, Matthias Kabatnik
University of Stuttgart, Institute of Communication Networks and Computer Engineering
Pfaffenwaldring 47, 70569 Stuttgart, Germany
{hauser, kabatnik}@ind.uni-stuttgart.de

Abstract

The fear of services building user profiles will constitute a rising threat to new mobile services. Especially when thinking of location based services, users must be able to trust the system not to misuse their location data. As the number of participants to new location based services will be likely to be very large, a scalable solution for controlling the disclosure as well as the linkage of users' location data to their identity will be needed. We develop a privacy architecture for a global location service, permitting users exactly to define who will get which granularity of location data as well as identity information. Our architecture reduces necessary trust in the location service and prevents linkage of location queries even without encryption of the whole communication resulting in better performance.

Keywords: Security, Privacy, Location Service, Location Based Services, Authorization Certificates, SPKI, Authentication

I. Introduction

Location Based Services (LBSs) in general are services, that exploit knowledge of the current location of a service user. In some scenarios LBSs additionally need to know locations of other users in order to provide their functionality. Today's best known example is "E911" in the US, where the mobile phone operator has to determine users' location in case of an emergency. In Germany other LBSs have come into existence in the field of city guides or traffic telematics, e.g. the Tegaron service [1]. Examples are navigation services, where the current location of the car is taken into account for path determination or warnings of traffic congestions, actually affecting the user, as well as calls to the nearest garage in case of a car breakdown. First proprietary services are currently starting for determination of, e.g., the nearest Italian restaurant, subway station or whatever. Future is expected to bring much more sophisticated services. Within the scope of the research project NEXUS [2] we are developing an open global platform for all kinds of spatially aware applications.

It is commonly assumed that location based services are going to be the so-called "killer application" of 3G wireless networks. This is reasonable since mobile phones have a high market penetration and the enhancement of future mobile terminal equipment by positioning capabilities is expected. There will be terminals with an integrated GPS receiver as well as other possibilities of locating a mobile user (e.g. Time Difference of Arrival, TDOA). On the other hand, small computing devices like pocket PCs or Personal Digital Assistants (PDA) are getting more and more spread in today's society. First products already exist, integrating mobile phones and PDAs. Computing power and integration will rise during next years and technology of today's notebooks is migrating into smaller devices.

After pointing out the technical reasons for feasibility of LBSs we want to look at properties of future mobile applications. In addition to stationary user behavior, a mobile user's needs are influenced by different environmental aspects. A mobile user, not attached to his home network is likely to be interested in information about his (unknown) environment and will need services related to his mobility (e.g. navigation). Furthermore he does not want to browse the Web for a long time, searching for information about his current environment, because of low and expensive bandwidth on the wireless link. A LBS takes the location of the user into account automatically.

Moreover relationships between users often depend on the area the users are in and must be passed to the service as parameters.

One important point of criticism regarding LBSs in general, is the users' fear of total surveillance, the so-called "Big Brother" scenario. The mobile device is considered to become an always-on universal assistant of the user in totally different aspects of life. Possible examples include (geographically targeted) E-Mail, online-banking, -brokering, -trading, scheduler, speech or voice recognition services in the infrastructure, navigation and other traffic telematics services as well as explicit location queries. Regarding the whole range of applicability, there is strongly personalized data flowing to and from the mobile device.

Because of the diversity of applications, it would be possible to collect a nearly complete user profile which furthermore does not have to be collected by a complicated distributed observation but just by simple data base queries.

Looking at privacy threats of location aware systems in general there are a lot of standard problems of distributed systems, like protection of communications as well as problems of authentication and authorization. However, the main new threat which is LBS specific, is the combination of a user's location and identity information. Knowing a user's location often permits inference of his activities as well. Even if this could be just an imprecise inference in some cases, one would hardly agree to let anybody know, that one is in a dubious area even if the possibility of a straight walk through is well given.

A more general threat is constituted in the new scenario among service providers. In most of today's scenarios, cellular phone network operators provide a full range of services, i.e. basic transport and value added services. Although there is collaboration between different operators (e.g. roaming) the scenarios are still monolitic with respect to administrative domains. In near future more heterogeneous scenarios are expected. Networks will have to be opened for services of other providers (third party provision). Thus, trust models considering one trusted provider only, no longer hold, requiring more sophisticated protection of user data than offered by today's systems. Moreover, within LBSs the need of a well controlled disclosure of sensitive location data to distinct services must be considered.

One of the main problems regarding launch of location aware systems like NEXUS lies in finding a privacy model and an architecture a possible user is willing to trust. A key requirement therefore is, that a user must be able to fully control disclosure of his location data, i.e., that nobody will gain any information about him without explicit allowance.

So far, we just considered privacy needs of a user, but the interests of other parties must be taken into account as well. Service providers also have to be protected, e.g., against threats from users acting as attackers as well as from malfunctioning devices. Moreover a user can act as a service provider with respect to his own location data, offering it to other users and network services.

Looking at all security and privacy needs, there will often be a conflict between needs of a user and those of a provider which has to be solved by negotiation. For automation of that, machine readable policies and negotiation mechanisms are needed which also need to be readable by or at least easy preparable for displaying to users.

In this paper we will focus on protection of location information (LI) within the example of NEXUS and its location service (LS) [3]. Nevertheless, our results will be usable for any global location service. As future location aware services need more accurate location information than mobile telephony providers nowadays have (i.e. the cell, in which the user is roaming), more and better location sensors are needed. In NEXUS we think of location sensors attached to the client device, e.g. GPS, as well as of sensors in the infrastructure like improved cell information from the mobile telephony providers. This sensor information is aggregated in a global location service, so that in principle the highest possible accuracy is available there.

In chapter II we are deriving requirements for an access control (AC) of a global location service for NEXUS or other LBSs. In chapter III fundamentals for our proposed architecture, presented in chapter IV, are described. At the end of this paper our approach is evaluated and topics of future research are outlined.

II. Requirements for a global location service

Considering an open and global platform, permitting everybody to participate either as a provider of location information or related services or as a user of these services, a large number of communication events can be anticipated. On the one hand there are many subjects, which may issue location queries and on the other hand there are many targets which can potentially be located. In the remainder of this paper we refer to this naming, that "subjects" issue queries about the location of "targets". If LBSs become the killer application for new mobile networks, a high percentage of the users of existing cellular networks are likely to participate—having location entries in one or more location services and issuing location requests. This magnitude of users will result in a large

number of location queries. Furthermore, regarding access rights these users have, we have to take into account that relationships among people will change frequently, up to several times a day. Considering a usual scenario, I want my colleague to be able to locate me at office hours, but just at the time, I leave office, I do not want him to know my position any more. Perhaps we meet in the evening and then I want him to locate me again.

Taking these requirements into account, we state that a static access control cannot fit our needs. A static access control list (ACL), e.g., would be far too big to be stored in a consistent way and to be processed in an acceptable speed. Thinking of a mandatory access control, it would probably be impossible to assign all subjects and targets to an ordered set of long-lived security labels. Each change of a relationship between a subject and a target would result in a change of the ACL or a new classification of either one. In [4] the author has combined mandatory and discretionary principles, nevertheless resulting in large and static structures. Instead we need a very dynamic access control for the location service.

Because of the large number of expected queries one of the main criteria regarding the location service is performance in processing queries. Hence, performance is a main criterion for the privacy functions as well.

So far requirements regarding a global large-scale location service were derived, in this section we will extent our approach to the access control in a LS that does not have users' full confidence. One major design goal of our architecture is a low traceability of a user's location profile even from the viewpoint of the LS. Although the user has to trust the LS with respect to correct functionality—especially of security functions, e.g. the access control—this trust can be limited by reducing the information about the combination of identity and location data of a single user (Data Economy). Thereby the amount of information stored in the LS shall be under the user's control.

In principle there are two parameters to control this

- accuracy (frequency) of location updates
- the identifier assigned to the target with the LS

The first approach is to enable control of sensors to just report location information with a tunable accuracy to the location service assuring that nobody is able to obtain more accurate information. Considering location sensors attached to the target's mobile device, like, e.g., a GPS sensor, this is very easy to realize. It is more difficult to control accuracy of location data delivered by external sensors like e.g. the bluetooth cell. The main drawback of this approach is that no differentiation between users is possible. The restricted accuracy has impact on all users in the same way. This limits the usability of the whole platform significantly.

The second possibility is to give limited information about the user's identity to the LS. This can be achieved by using a pseudonym as the LS's reference to the user. The amount of information about the user's identity or other user related properties can be limited. Thus, the LS may be permitted to have very accurate location information. Nevertheless trust is necessary when the LS is in charge of controlling the accuracy of information answering other entities' requests according to the rights given to these subjects by the target. The second approach is preferable because of its flexibility though injecting more complexity in location service's AC. Nevertheless, users who do not want to be located by anybody still can control the maximum accuracy of the information passed to the LS by the sensors.

Moreover, if the LS would know its targets by their real identity, these identities must be presented to a subject within the answer to an Area Query, wherein a subject requests what targets can be found within the specified area (e.g. a polygon).

Even if the target provides a pseudonym which has to be used by the LS within the context of Area Queries, other users and services still can track the history of LI under this pseudonym. In case the pseudonym is revealed, the complete history of LI bound to this pseudonym is disclosed to a potential attacker. This might especially happen in the case of collaboration with the LS.

Hence, we can conclude that it must be possible for a target to register at the LS with a pseudonym if the location service shall be able to provide most accurate location information allowing the platform to be used in a flexible way.

The pseudonym used as reference within the LS must not be revealed within any request of a service user to prevent linkage of actions and location profiling within this context. Additionally, a subject who wants to locate a target needs a temporary reference to the target's entry which is unambiguous but not linkable to other temporary references to the target's entry given to other users. Since the LS must be able to resolve the temporary reference to the pseudonym of the user to look up the location data, this reference must contain data from which the LS pseudonym can be derived but must be unreadable for all other parties.

As relationships between users or between users and services, and accordingly permissions the users and services have, change very frequently, a global location service has to have a dynamic access control. It is preferable that the users are able to give permissions directly to other entities without involving any administrator or changing parameters of the LS's access control using a management

interface. Furthermore it is required that no access to location information of a specific target may be possible unless prior authorization by this target.

In case a service queries location information on behalf of a user, the rights of the original caller, i.e. the user of the service, must be effective parameters for the access control decision function.

III. Background

After introducing privacy issues of LBSs as well as inferring main requirements for an access control of a global location service, we will describe some fundamental mechanisms and principles needed for our approach to ensure privacy of location data. As said before, there are two possibilities for dealing with the undesired linkage of identity and location information. On the one hand, we can control the amount of disclosed identity information and on the other hand, we can control the accuracy of disclosed location information.

For controlling the granularity of location information, there are several possibilities, e.g., rounding or truncating. To reduce the accuracy a random error might be added to the real position. These mechanisms can also be combined. An evaluation of these mechanisms is beyond the scope of this paper.

Controlling the amount of disclosed identity information is more difficult, because it is not possible to do any numeric calculations on identity information and add, e.g., a random error. Instead, a target uses several identifiers, typically one identifier for each partner it is in contact with. To each identifier additional information can be bound like, e.g., the real name, the private address or the business address. Without the name provided the identifier is a pseudonym.

Thus, depending on the chosen pseudonym a user is able to disclose more or less personal information. While using a service sharing a specific pseudonym, a user exchanges more personal data which in future can be linked to this pseudonym. If too much information is disclosed, the user needs to create a new pseudonym making no more use of the old one. This kind of identity management has to be supported by the client device, which should keep track of the ongoing disclosure and remind the user, when a new pseudonym has to be used. While NEXUS is a platform for many different services and thus many pseudonyms are needed and sometimes linkage of transactions of a specific pseudonym is wanted, we do not consider a periodical renewal of pseudonyms like proposed in [5] resulting in anonymity. Since this topic exceeds the scope of this paper, we refer to the literature, e.g., [6].

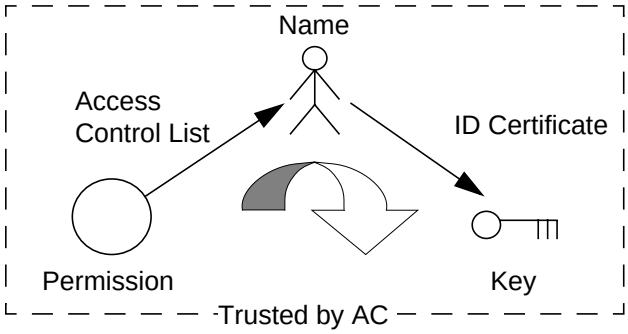


Fig. 1: Authorization flow with name as identifier

Having mentioned some principles how to control the amount of disclosed information above we will now show some fundamental mechanisms for controlling who gets permissions to what amount of data, according to [7]. As our approach is based on asymmetric key cryptography, let us first have a look at the relation between a user and his key pair and therefore at the difference between a handwritten and a digital signature, both assuring some kind of integrity. A handwritten signature can be regarded as a biometric proof, because of the dependence on biometrical properties of the signing person. As we can identify the person, who signed the document, we cannot assure this document not to be changed afterwards. In contrast, a digital signature can proof the document's integrity even if it was in untrustworthy hands in the meantime but it tells only, that the owner of a given private key has signed it. The digital signature can be viewed as a stamp. Everybody being in account of the private key can issue it and nothing about the identity of the signing person is said as long as no additional information is available, e.g. a certificate binding some attributes, e.g. an identity, to the private key.

Looking at an access control operating with authentication based on public key cryptography, the public key of the requesting user has to be known. To non-ambiguously map the key to a person an identity certificate must be known, too. The AC initially does not know what permissions this user has. This knowledge has to be provided by the AC's administrator, e.g., in form of an access control list. Permissions in an ACL are usually given to a person described by its globally unique name. The AC has to use the name corresponding to the key, used to authenticate the request, in order to determine which permissions this person has. In fig. 1 the flow of authorization via the person's name to the key is shown. In this scenario, the AC has to trust every participating instance, including the identity certification authority, assuring the binding of name to key, because every information is elementary important for the access control decision.

For authorizing a specific person a globally unique identifier is needed. So for authorization by name, this one has to be globally unique, like e.g. hauser@ind.uni-stuttgart.de.

Nevertheless another globally unique attribute is a user's public key which is tightly bound to the user owning the corresponding private key. Thus a user's public key can be used for authorization, too, allowing to bind the permissions of an ACL directly to the key omitting the need for a name in the scope of an access control decision.

Using a public key as principal no identity certificates are needed anymore and no identity certification authority trusted by the access control is needed either. In some cases however identity will be required, but rather for lawyer's security or for tracking down a fraudulent user and not for access control decision. This results in a trust model depicted in fig. 2.

By using public keys as identifiers, we obtain a reduced number of trusted parties and better performance of the access control in means of communication and computation, because of the omitted need to resolve the name. Moreover as depicted in [8] no global trusted third parties or global name spaces are necessary which constitute a single point of failure as well as trust problems. As no global hierarchical structure is enforced openness and scalability are improved. In the next section we present a mechanism for achieving a dynamic AC according to [8], [9], [10].

Authorizations of a keyholder do not have to be statically stored in an access control list but can also be issued by a so-called authorization certificate, which binds the permissions of the keyholder directly to its public key. Therefore the issuer of permission passes a certificate to the authorized subject. The certificate lists the explicit permissions together with the subject's public key, proven by the issuer's digital signature. Thus the owner of the information to be controlled is able to issue authorization on its own, without involving any administrator. An authorization certificate can be viewed as a formal document of local trust relationship, nevertheless with global validity, between the issuer and the subject receiving this certificate.

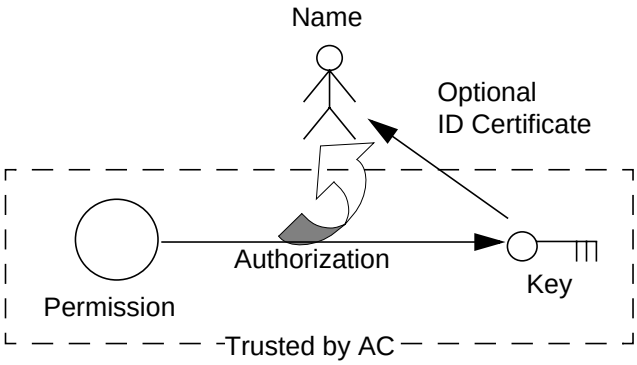


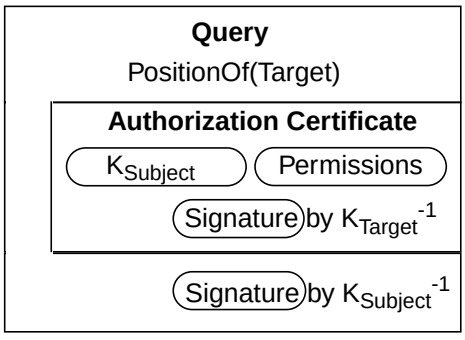
Fig. 2: Authorization flow with key as identifier

The certificate authorizing the public key is presented to the AC together with the subject's query which is signed using the corresponding private key as depicted in fig. 3. On reception, the access control has to check, whether the signer of the query is identical with the subject authorized by the certificate and whether the signer of certificate is allowed to issue permissions for the target, whose location data is queried. Both of these operations are simple key comparisons. Thus, the access control function is getting the querying public key's permissions just in time and does not have to store it permanently. This mechanism provides a decentralization of authority and management operations, while sticking with the principles of discretionary AC and permitting users to allow or restrict access to others on their discretion.

With the use of authorization certificates, we omit the use of very large and static access control lists. Principally the ACL just needs to contain those entities which are authorized to sign certificates for a specific target, in most cases this will be just the target itself. Authorization certificates are based on public key cryptography, i.e. a subject's public key is used as identifier as well as use of the issuer's private key for signing the certificate. Thus, integrity is provided and the certificate can be transmitted even by untrusted third parties, e.g., being delivered by the Internet.

IV. Access control architecture

In the previous chapters, requirements for the access



K_{Target}^{-1} ... private key of Target
$K_{Subject}^{-1}$ ... private key of Subject
$K_{Subject}$ ... public key of Subject

Fig. 3: Query with authorization certificate

control as well as technical fundamentals were given on which our architecture is based. By use of authorization certificates we principally achieve scalability as well as dynamics of the access control. Impossibility of linkage of location queries and pseudonymous usage, lowering required trust, of the location service is achieved by the following means.

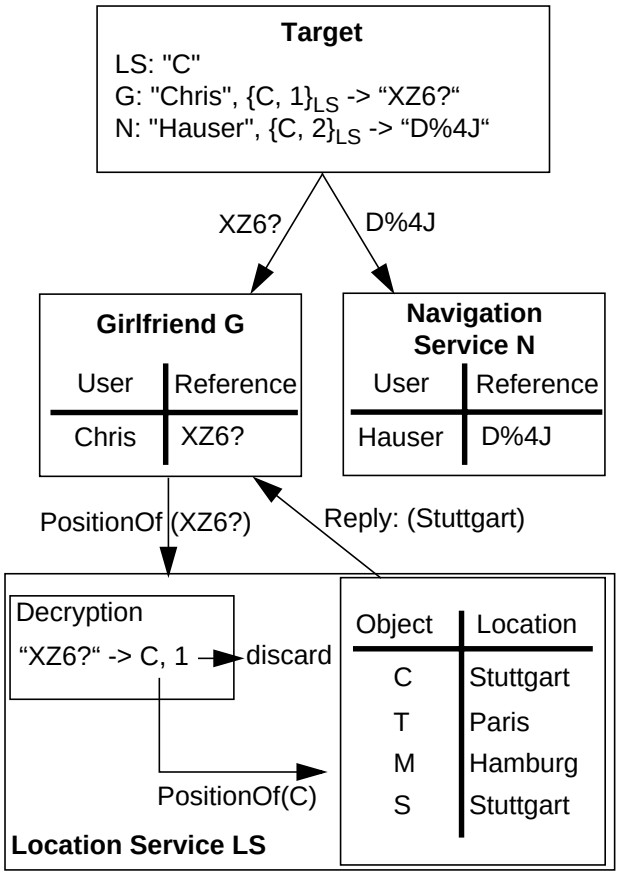
The main idea of our concept is to use an asymmetric key as a pseudonym within the LS. This key is known by the LS and the target only. The knowledge of the corresponding key is limited to the target itself. In the following we give the pseudonym key the name “C“. A subject authorized to get the position of a specific target, has to be able to address that target in a query. Because the subject does not know “C“, this pseudonym has to be passed to the subject once, e.g., when issuing the authorization certificate. It is important, that the subject is not able to read this pseudonym. This can be achieved by encrypting it with the public key of the location service resulting in a tunneling of the pseudonym “C“ from the target to the LS. Thus, the encrypted pseudonym serves as a kind of reference, with which the subject can address the target in location queries.

To prevent an external attacker from matching queries of different subjects to the same target, the appearance of the ciphertext of the location service pseudonym “C“ has to be different for different subjects. This is achieved by encrypting “C“ together with a unique piece of information which is chosen individually for each subject. If some queries may be linked, e.g. because they belong to the same communication session, the same reference can be used. As soon as linkage of queries has to be prevented, a new reference with a new additional information has to be generated. On reception the location service decrypts the ciphertext of the reference, used as address, and discards the latter part of it. This additional piece of information does not need to contain any information from the addressing point of view, what in fact even has to be avoided since the target therein can pass any information to the location service, which is carried but not seen by the subject. Moreover this part has to be well defined in order to avoid buffer overflow attacks.

In fig. 4 an example of a Position Query is depicted, with a target, that wants to be located by two subjects, say its girlfriend “G“ and a navigation service “N“. The target uses the pseudonym “C“ as reference with regard to the location service, the identifier “Chris“ towards its girlfriend and the identifier “Hauser“ when communicating with the navigation service. For simplicity, the authorization certificates, which have to be attached to queries, are omitted in this example. The target produces two references for G and N, encrypting the LS pseudonym together with a unique piece of information for each subject, “1“ regarding G and “2“ regarding N, using the public key of the location service. The encryption is depicted as {pseudonym, unique information}$_{LS}$ resulting in references named “XZ6?“ and “D%4J“. If the girlfriend wants to know the position of the target, which is known to her as “Chris“, she is issuing a Position Query to “XZ6?“. The navigation service issuing a Position Query would indicate the target, which it knows as “Hauser“, by “D%4J“. A possible attacker would not be able to link these two queries the one about “XZ6?“ and the one about “D%4J“ to the same target, even when using an unsecured communication. The LS decrypts the reference “XZ6?“, discards the additional piece of information (“1“) and queries its data base about the position of “C“. At last the reply “Stuttgart“ is sent back to the girlfriend.

Since access rights are granted with respect to targets but not areas, authorization of Area Queries is less straight forward than that of Position Queries.

First it is possible to operate in a kind of anonymous mode. Every object can specify a pseudonym, that has to



{C,1}$_{LS}$ ... encrypted with public key of LS

Fig. 4: Pseudonymous Position Query

be used when an Area Query is answered. This might be an arbitrary name or a certain role, e.g., the role of pedestrian which forms a certain anonymity group. It is even possible to remain invisible if the requestor does not have any permission. This is up to the policy of the service provider and to the target itself.

In case the service user wants to request whether a set of certain targets is located within a given area, it is not possible to simply pass one certificate describing the authorization to query a specific area. Rather, the subject has to pass the authorizations for LI of all relevant targets potentially roaming in that area.

If the selected area is too large to give a full list of objects the LS may suppress a detailed report of anonymous objects giving just information on targets requested explicitly.

In fig. 5 an example of an Area Query to “Stuttgart“ is depicted. The girlfriend “G“ from the upper example attaches the authorizations which are valid in the queried area, these are Cert.1 concerning “Chris“ and Cert. 3 permitting query of “Matt“. The location service checks, which objects are in the queried area and for which the authorizations of “G“ hold. It answers with numbers, according to the position of the certificates in the query, of those targets roaming in Stuttgart. On the one hand, the LS does not know the identifiers “G” knows and on the other hand communication load is decreased by just transmitting numbers. In our example, “C“, who is target of Cert. 1 and “S“, for whom “G“ does not have any permission and who so far is visible as “anonymous“, are roaming in Stuttgart.

As we think primarily of mobile devices when discussing location based services and NEXUS, it could be a drawback to transmit many certificates across the wireless link. Therefore, certificates should be kept small e.g. by applying compression. Besides, in the majority of the cases a subject would not have too many valid permissions in a given area. Anyway there are some ideas to alleviate this possible drawback. There are, e.g., more sophisticated algorithms possible to select certificates to be attached or a trusted entity connected to the internet by a broadband link, e.g., the user’s Mobile IP home agent or perhaps some trusted part of the location service can take care of the certificates that can be registered prior to a location request. These scenarios are subject to further work.

Since we use asymmetric keys as principals and the key used as pseudonym within the LS has to remain concealed there must be mechanisms to establish trust between subject and target with respect to the asymmetric keys and the reference respectively.

For enabling the target to trust the key of the subject which wants to be authorized it is possible to use identity

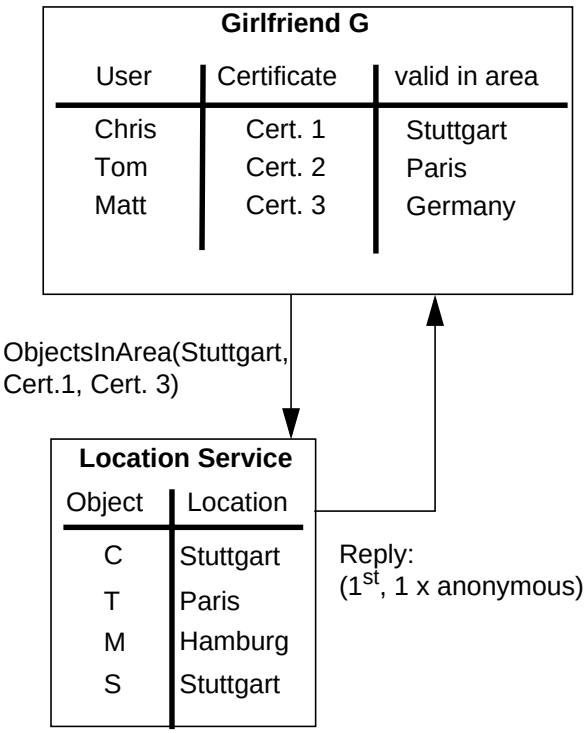


Fig. 5: Area Query

certificates signed by a trusted third party (TTP) binding the subject’s name to its key, presuming the target knows this name. This TTP has just to meet the trust requirements of the target and does not have to meet those of the location service’s access control, so it could, e.g., be a local instance knowing both, target and subject. Moreover, in many cases target and subject will already have a relationship external to the system, perhaps a friendship or a business relation, so they know and trust each other when exchanging keys directly. With respect to this question of trust, the user application has to display exactly what is known about the subject, e.g. a local name, a postal address or an address of a network controller, in order to facilitate even for an unexperienced user to make a good decision, that meets his security goals.

Secondly, the subject has to establish trust in the target’s reference. The subject is receiving a ciphertext which is said to be an encrypted pseudonym of the target. Since the reference is a part of the access right granting certificate signed by the target, there is a possibility to verify its correctness by presenting it to the LS which can check the signature and compare it to the asymmetric key within the reference. Therefore, an online verification interface is provided by the LS.

For authenticating the encrypted pseudonym, a possibility is needed to verify, that the location service accesses

indeed the correct target's information by that reference. This could, e.g., be achieved by a check of the reply to a Position Query, while seeing the target in reality. Nevertheless, in many cases, authorizations and encrypted pseudonyms are exchanged, while not seeing the target. For these cases, a more general approach using just the technical system is needed. These authentications have to be further developed and validated in future research.

V. Conclusions and further work

In this paper we outlined an architecture for an access control of a global location service like the one of the research project NEXUS. We showed, how authorization is spread with help of certificates achieving scalable access control lists in the location service as well as avoiding frequent use of the service's management interface and how the need for a global trusted identity certification authority of identity can be avoided by using asymmetric keys as pseudonyms. Because the keys used for public cryptography have to be rather large (e.g. 2048 Bit) it could be used a collision free hash over the public key as identifier. This approach attains decentralization of management as well as authority operations and furthermore fulfills the paradigm that without a first contact with a target, where the reference is passed, no query about this target is possible, which will raise user acceptance of location based systems in our point of view.

Moreover we showed, how a location service can be used without fully trusting it. One has to trust the service with respect to correct functionality, but we decrease necessary trust in the AC's administrator as authorizations are issued by the target itself rather than by an administrator. Furthermore we avoid the need to give one's real identity to the location service by enabling to use it pseudonymously permitting use of a unique pseudonym for the location service. For authorizing a sensor to report the location of a user with a specific accuracy, this sensor can get an authorization certificate, which he has to present to the LS when updating the user's location, achieving control of maximum available accuracy. Moreover, we showed that this architecture is applicable for both basic query types, Position Query and Area Query.

Openness as well as scalability are achieved and linkage of location queries is prevented, obtaining a better performance as not the whole query has to be decrypted by the LS. As an attacker is not able to link an observed query to a specific target and especially to link several queries to the same target, he is not able to gain more knowledge than he already has. So we can avoid easy gain of knowledge by simple observation of a link or a service. Of course several subjects are able to collaborate on a higher level, meaning the users can talk to each other or exchange information in another way, but this cannot be considered by any technical system. Nevertheless, a user is able to stop any linkage of information by deregistering and registering again with a new pseudonym as reference in the location service.

A man in the middle, receiving a query and thus getting in possession of an enciphered pseudonym which he can use for further queries, is not able to get much information about the target's location as he does not have any authorization. The authorization certificate attached to the intercepted query authorizes the key of the real requestor and as the attacker is not in possession of the appropriate private key, he may not sign further queries using this certificate. The attacker would even not know the queried target, because the enciphered pseudonyms are not linkable to any target. Additionally the location service's response can be encrypted with the public key of the authorized requestor, so a man in the middle even could not read the response.

A possible weakness of the outlined approach is revocation of issued permissions, as "no permission" cannot be expressed. The easiest solution are short lived authorizations, which have to be renewed frequently, in order to keep the interval of potential fraud in limits. Another possibility is a kind of authorization revocation list in the access control which can be modified by the targets. Furthermore, a target can specify a globally valid maximal accuracy to be queried by any subject. Evaluation of a solution is subject to further work, same as remedy of the possible high overhead on the wireless link by many attached permissions to an Area Query.

How users in their different roles can establish trust as well as a prevention of the possibility to pass some information within the encrypted pseudonym, to the location service, which is carried but cannot be seen by the subject, are topics of future research, too.

A problem, which cannot be solved by any mechanism is that a user can reveal his private key, what would constitute a problem to any system based on asymmetric cryptography. Furthermore, the users have to be aware of the consequences when issuing permissions. Both problems require awareness of underlying problems, which has to be assisted by good training as well as good user interfaces which have to be carefully evaluated with the assistance of, e.g., sociologists.

Another important aspect which is out of the scope of this paper is inference with knowledge of channels used for service related communications. Network addresses might reveal—from an observer's point of view—additional information about a user's identity and/or location.

Besides all considerations in this paper, trust in cor-

rectness of location information is still essential, since it will always be possible for a user to report malicious positions by just faking a location sensor or by not taking the sensor with him. Therefore a mechanism must be found for the location service to detect the correct information or a rule, which sensor to prioritize.

VI. Acknowledgements

This work was partially funded by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG).

VII. References

[1] **TEGARON Telematics**: http://www.tegaron.de

[2] **NEXUS - An Open Global Infrastructure for Spatially Aware Applications**: http://www.nexus.uni-stuttgart.de

[3] **A. Leonhardi, K. Rothermel**: *Architecture of a Large-scale Location Service*, Stuttgart, Institute of Parallel and Distributed High-Performance Systems, 2001.

[4] **U. Leonhardt, J. Magee**: *Security Considerations for a Distributed Location Service*, Journal of Network and Systems Management, Vol. 6, No. 1, September 1998.

[5] **D. Kesdogan, K. Reichl, K. Junghärtchen**: *Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks*, Proceedings of the 5th European Symposium on Research in Computer Security (ESORICS 98), Springer, Louvain-la-Neuve, September 1998.

[6] **U. Jendricke, D. Gerd tom Markotten**: *Usability meets Security - The Identity-Manager as your Personal Security Assistant for the Internet*, Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC 2000), pp. 344-353, New Orleans, USA, December 2000.

[7] **C.M. Ellison**: *The nature of a useable PKI*, Computer Networks, Vol. 31, No. 8, April 1999, pp. 823-830.

[8] **L.R. Rivest, B. Lampson**: *SDSI - A simple distributed security infrastructure*, April 1996.

[9] **C.M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen**: *SPKI Certificate Theory*, RFC 2693, IETF, September 1999.

[10] **T. Aura**: *Distributed Access-Rights Management with Delegation Certificates.* Secure Internet Programming: Security Issues For Distributed and Mobile Objects, J. Vitek, C. Jensen (Eds.), Springer, 1999, pp. 211-235.