Internet Engineering Task Force
Internet Draft

SIPPING WG
D. Trossen
Nokia Research
H. Schulzrinne
Columbia University
draft-trossen-sipping-ondemand-01.txt

24. August 2004
Expires: Feb. 2005

Ad-hoc Access Authorization for SIP Event Subscriptions

Status of this Memo

Copyright Notice

Abstract

A target or presentity may want to temporarily allow limited access to its location or presence information to a third party. We will describe in this document use cases and solutions (focusing on the delivery of geospatial information and presence). We will further outline the relation to ongoing SIMPLE and GEOPRIV work.

Table of Contents

1. Introduction

Access authorization for SIP event subscriptions is crucial due to the highly private nature of information revealed in the resulting notifications, e.g., all presence subscriptions must be authorized by the presentity. Work is currently ongoing within the SIMPLE and GEOPRIV working groups to define, manage and convey authorization policies for resource information such as geospatial information [1] and presence [8].

The policy documents envisioned in [1] are based on a three-step process. In the first step, the target or presentity composes a set of rules. In the model noted, these rules are encoded as a sequence of XML elements, each element representing a rule allowing comparison by user identity, time of day and other factors. These rules are, as a second step, uploaded to the presence agent (PA) or location server (LS). Since they have similar roles, we refer to this entity as a PA/LS. The protocol for uploading might be XCAP [9], among other choices. In the final step, the rules are applied when subscriptions arrive and when a notification is generated for a particular watcher.

It is important to note that policy documents may allow anonymous access, i.e., access that does not depend on the querier or subscriber to identify itself. In this document however, we are only concerned with identity-dependent access, i.e., where access depends on the identity of the entity requesting the information.

Most of the discussions for authorization have assumed long-term relationships between the entities requesting information and the target or presentity. However, there is a class of applications where the presentity or target wishes to grant temporary and limited access to its data to services. In this, the service might require a single or more than one sample of the location or presence information to perform its function. These services might transform the presence or location data into more useful renditions or use it to provide services that have little to do with presence or location. Section 3 discusses some examples of these services.

Several design alternatives are possible to tackle the above outlined problem of temporarily granting access to presence or location information. Section 4 discusses these design alternatives and their relation to the currently ongoing work in the SIMPLE and GEOPRIV working groups. While there exist solutions for most of

these design alternatives, we present in Section 5 a particular solution for one of the design alternatives.

2. Terminology

Resource: A resource in the scope of this document is an object to which a certain state information is associated, called æresource dataÆ in the remainder of the document. Examples are presence as a resource belonging to the presentity. The resource data is the

current presence information (subject to the particular disclosure policy of the presentity). Resources can also be associated to devices, such as printers, in which the resource data represents, for instance, the current state of the printer. In the context of the SIP event framework, the resource state is abstracted with SIP events and hosted at particular SIP event servers.

Resource owner: An entity that has authorization power over the particular resource data. Examples are presentities in SIP presence or rule makers as introduced in [1].

Information generator: An entity that determines or gathers resource data for a particular resource. Examples are publishers in SIP presence or location generators in GEOPRIV [1].

3. Use Cases

With the defined terminology of Section 2, consider that a subscriber S desires access to a particular resource D (or particular parts of the resource), such as presence or geospatial location information, at a particular SIP event server. In this, the desire for access is somehow conveyed from the subscriber towards the resource owner A. The desired access can be time-limited or limited in notifications (such as time window based, one-time or N-time notifications).

The following additional constraints might occur:

* The identity of the subscriber might not be known to the resource owner before the desire for access is conveyed towards the resource owner.
* The type of access, i.e., the resource as such as well as the resource data, might not be known to the resource owner before the desire for access is conveyed towards the resource owner.
* The conveyance of the desire to access the resource data and the actual access might lie within a rather short time window.

The problem to be solved is to enable an authorized access to the

desired resource by the subscriber at the SIP event server. It is worth mentioning that such authorized access is not restricted to currently discussed presence items only rather than to any kind of (future) presence items or SIP events in general.

Further note that it is beyond the scope of this document as to how the subscriber conveys the desire for access to the resource owner. A variety of methods, such as within an HTTP or SOAP transaction between subscriber and resource owner (see also the following use cases), are possible for such conveyance.

In the following, use cases are presented as examples for such temporary access to resource information.

3.1. Enhanced Location Services

Consider the provisioning of location-based services from a service provider (the subscriber S) to a user (the resource owner A).

As an example, Alice would like a mapping service S to create a map that plots her trajectory for a limited time period, For this, S needs access to location data, but only for a limited time.

3.2. Context-aware News Service

Alice subscribes to a news service that delivers news items adapted to her current activity, mood and location. In order to perform the adaptation, the news provider S needs to access particular presence items for the time of the news delivery (which can be rather temporary in cases where the content was found during surfing the Internet).

3.3. Service Discovery in Visitor Environment

Alice would like to discover services in a visitor environment (i.e., Alice and the discovery system most likely do not have an existing trust relationship), the service selection depending on her location, activity, currently used communication devices and other information. In order to perform the appropriate (context-aware) filtering of available services, the discovery agent requires access to AliceÆs information, such as presence or location.

3.4. Match Making Service

Alice temporarily subscribes to a match making service (e.g., within an amusement park or bar) that alerts its customers if two or more

compatible individuals are in close proximity. In order to perform the desired match making, the match making service provider might require access to certain user information, such as location within the point of interest (if the place is larger) or current activity.

3.5. Context-aware Gaming

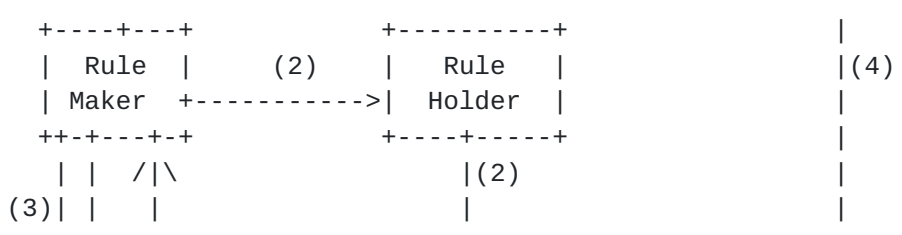
Mobile games combine players moving about in the real world with computer-mediated interaction. Such games require rich presence information, including sensor data representing activities (such as æstandingÆ or ækingÆ) and current location. All players have to be able to subscribe to the location of, say, their teammates. Such games could be established between a-priori unknown parties (ad-hoc gaming in point-of-interest for instance) but could also require a-priori unknown set of information from either player.

Hence, upon starting the game, each player requires access authorization for this particular set of information from each of the other players for the duration of the game (if the duration of the game is unknown, the authorization can be renewed before expiring).

4. Design Alternatives and Relation to SIMPLE and GEOPRIV Work

As said in the introduction, different design alternatives exist to tackle the problem of temporarily granting access to presence or location information. This section outlines these design alternatives in the context of ongoing SIMPLE and GEOPRIV work in the area of access authorization for SIP events.

The following picture outlines the relation of the different design alternatives to this ongoing work. For this, we use the GEOPRIV architecture as introduced in [1]. However, for the sake of generality the entities are named independent of the particular resource data, i.e., the information generator equals the location generator in [1], while the SIP event server equals the location server and the SIP event subscriber the location recipient in [1]. The SIP event subscriber in this figure is similar to the service provider in the use cases.



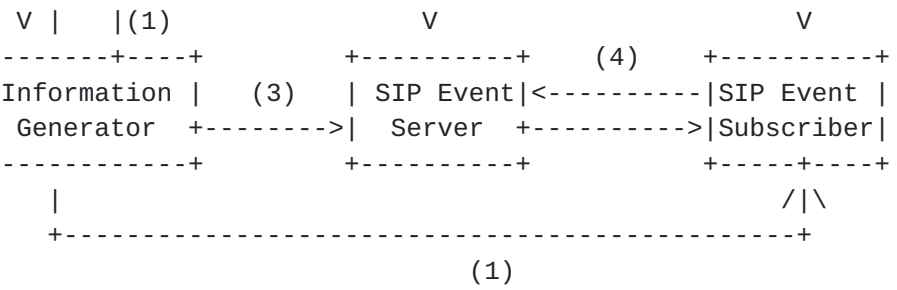


Figure 1: Design Alternatives And Their Relation to Ongoing Work

Figure 1 shows four different alternatives to tackle the problem of temporarily granting access to the desired information. These alternatives are discussed in the following.

4.1. Data Push

In data push mode (alternative (1) in the figure), resource owners do not allow subscriptions at all. Rather, the rule maker simply delivers the desired resource information (after having the information obtained from the information generator), e.g., presence or location data, via, e.g., SIP MESSAGE, to the service provider. This mode offers the presentity/target (P/T) complete control over data delivery, but otherwise has little to recommend it. It requires that the P/T establish an authentication relationship with the service provider so that the service provider can know who is submitting data. The P/T has to guess how often the service provider needs updated data. Finally, this method is not very bandwidth

efficient for mobile P/Ts as, e.g., they may need to obtain location data from a location generator and then transport the data again over the same air interface, possibly in multiple copies to multiple service providers.

4.2. Policy Conveyance via Rule Holder or directly to SIP Event Server

In case (2) of the figure above, the rule maker defines the appropriate authorization policy and conveys it to the rule holder using, e.g., XCAP operations [4] for upload. The authorization policy is then pushed to or pulled by the SIP event server, e.g., using the XCAP event package [5]. Incoming subscriptions then use the available authorization policy information to grant or deny the subscription.

In case (3) of the figure above, the rule maker is publishing the authorization policy directly to the SIP event server via the information generator. The conveyance from the information generator to the SIP event server usually happens during the publication of

the particular information itself to the SIP event server.

In case of a temporary access, both schemes require additional steps in order to cope with the temporary character of the desired access:

(1) Create a new identity for the subscriber S or ask S for the identity it wants to use in the subscription to the data. (A may only know S as a web page, so it cannot necessarily guess the user identity.) There does not appear to be a standard protocol for this step.

(2) Create a policy rule that allows appropriate access for the particular resource information by this identity.

(3) Create a user-password entry so that S can authenticate itself, e.g., via Digest authentication. The password can be created by S or A, but in either case needs to be exchanged securely.

(4) Remove the rule when S no longer needs access, to avoid inflating the policy information at the SIP event server and rule holder.

This approach clearly works, as it corresponds to the normal mode of managing subscribers. However, it incurs significant complexity and is particularly inefficient in mobile environments.

4.3. Policy Conveyance from Rule Maker to Subscriber

Alternative (4) in the figure above outlines the policy conveyance from the rule maker directly to the subscriber, then to be used in the particular subscription. As a simple solution, the rule maker could send the subscriber a subscription URI that includes the authorization policy, such as

sip:alice:Z@example.com

where Z is the encrypted authorization policy and alice@example.com is the rule makerÆs URI. The subscriber will use the provided subscriber URI in its subscription. This approach only works if the policy is relatively simple, e.g., a selection of standard data profiles combined with a time limitation.

5. Protocol for Policy Conveyance Within Subscriptions

The design alternative in Section 4.3 outlined the conveyance of the (temporary) access authorization policy from the rule maker directly to the subscriber. The suggested usage of a subscription URI that includes the (encrypted) policy bears the problem of allowing only simple policies. To overcome this problem, this section outlines a

protocol for conveying the particular policy as part of the SUBSCRIBE message body itself.

The protocol operation is divided into three steps, explained in the following.

5.1. Conveyance of Authorization Policy towards Subscriber

The first step is concerned with generating and conveying an authorization policy towards the subscriber for the particular information.

For that, the rule maker, according to Figure 1, generates such authorization rules for the particular pieces of resource information that are desired to be accessed by the subscriber. The rule maker signs the authorization rules description for authenticity and conveys the signed authorization information towards the subscriber.

It is beyond the scope of this document how the rule maker obtained knowledge as to which information the subscriber desires to subscribe to (usually, certain service interactions with the subscriber will convey such knowledge beforehand, such as web page interactions). Further, the protocol that is used to convey the signed authorization policy from the rule maker to the subscriber is beyond the scope of this document. Candidates for such operation are HTTP or SOAP.

AUTHOR NOTE: Details of protocol operation, such as for signing, and exact referencing of the XCAP application usages are still missing.

5.2. Subscriber Generation of SUBSCRIBE Requests

After the subscriber in Figure 1 received the signed authorization policy for the subscription, it will include this authorization policy in future subscriptions according to the provided authorization policy.

For that, the subscriber will include the signed policy in the message body of the subscription, in addition to event package

specific information, such as presence document information, according to RFC 3265 [7] (i.e., using multi-part bodies).

AUTHOR NOTE: Details of protocol operation, such as inclusion of policy in message bodies, are still missing.

5.3. Notifier Processing of SUBSCRIBE Requests

The notifier will process incoming SUBSCRIBE requests according to RFC 3265 [7]. If the inclusion of the signed authorization policy in the message body is indicated, the signed policy information is extracted from the body.

The extracted policy information is then forwarded to the rule holder (see Figure 1).

The rule holder verifies the signature of the received authorization policy. If the verification has been successful, the authorization policy is deemed valid. The success or failure of the verification is signaled to the notifier, which in turn grants or denies the submission appropriately.

AUTHOR NOTE: Details of using protocol between notifier and rule holder is missing. Is this in scope of the document?

6. Open Issues

* Verification Step: Is the protocol between notifier and rule holder for verification purpose within scope of the document? What are candidates for this protocol?
* Usage of authorization policy: After the authorization policy was verified by the rule holder, is the answer simply conveyed back to the notifier or is the policy used otherwise. One could see the authorization policy as implicitly defined (and verified) and the rule holder could add the policy to its current policy document. Or we use it for THIS subscription only and discard the policy at the rule holder after verification.

7. Security Considerations

A solution for the problem described in this document shall allow for granting access in ad-hoc authorization scenarios as described in Section 3.2. In this, any solution should allow for

* defining all relevant resource information in the authorization,
* tying the access to a particular querier, if so desired by the resource owner,
* preventing re-usage of the authorization through the querier or third parties,
* preventing disclosure of the authorization to third parties
* tying the access to a particular (relative or absolute) time window, if so desired by the resource owner, and
* verifying the identity of the resource owner.

These security considerations have been identified and are addressed

through the mechanism presented in Section 5.

8. Acknowledgements

The authors would like to thank Dana Pavel for her input.

9. References

[1] J. Cuellar et al., "Geopriv Requirements", RFC 3693, Internet Engineering Task Force, February 2004.

[2] H. Sugano, S. Fujimoto, et al., "Presence information data format (PIDF)", Internet draft, Internet Engineering Task Force, (work in progress), May 2003.

[3] S. Bradner, "Key words for use in RFCs to indicate requirement levels", RFC 2119, Internet Engineering Task Force, March 1997.

[4] J. Rosenberg, "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", Internet Draft, Internet Engineering Task Force, (work in progress), May 2003.

[5] J. Rosenberg, "A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents", Internet Draft, Internet Engineering Task Force, (work in progress), May 2003.

[6] H. Schulzrinne (ed.), "RPID -- Rich Presence Information Data Format", Internet Draft, Internet Engineering Task Force, (work in progress), July 2003.

[7] A. Roach, "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, Internet Engineering Task Force, June 2002.

[8] J. Rosenberg, ôA Presence Event Package for the Session Initiation Protocol (SIP)ö, Internet Draft, Internet Engineering Task Force, (work in progress), July 2003.

[9] J. Rosenberg ôThe Extensible Markup Language (XML) Configuration Access Protocol (XCAP)ö, Internet Draft, Internet Engineering Task Force, (work in progress), February 2004.

10. Authors' Addresses

Dirk Trossen
Nokia Research
5 Wayside Road
Burlington, MA 02474 USA
Email: dirk.trossen@nokia.com

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027 USA
Email: schulzrinne@cs.columbia.edu

Intellectual Property Statement

Full Copyright Statement

TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC editor function is currently provided by the Internet Society.