SPEERMINT WG
Internet-Draft
Intended status: Standards Track
Expires: November 10, 2007

A. Houri
IBM
E. Aoki
AOL LLC
S. Parameswar
Microsoft Corporation

May 9, 2007

Presence & IM Use Cases
draft-ietf-speermint-consolidated-presence-im-usecases-01.txt

Status of this Memo

Copyright Notice

Abstract

The document describes several use cases of peering between two or more service providers that provide none VOIP based collaboration services and presence and IM in particular. These service providers create a peering relationship between themselves thus enabling their users to collaborate with users on other communities. The target of the document is to drive requirements for peering between domains that provide the none VOIP based collaboration services.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

2. Introduction

Real Time Collaboration (RTC) services are becoming as prevalent and essential for users on the Internet as email. While RTC services can, like email, be implemented directly by users in a point-to-point fashion, they are often provided for or on behalf of a community of users within an administrative domain. As the use of these services grows, users increasingly have the need to communicate with users not only within their own community but with those in other communities as well. In practice, each community is controlled by some authority, and so there is a need to provide for easier establishment of connectivity between communities, and the management of the inter-community link. This document contains a set of use cases that describe how peering between communities may be used in none VOIP RTC services. The use cases are intended to help in creating requirements that will enable more secure and easier peering between communities that provide none VOIP RTC services.

This document will use the terminology as defined in [2] unless otherwise is stated.

The following sections provide several use cases followed by a discussion on what these use cases may imply regarding the functionalities that need to be provided for in order to implement those use cases

3. Use Cases

3.1. Simple Interdomain Subscription

Assume that we have two peer networks [2], peer network A and peer network B. User Alice@A.com wants to subscribe to user Bob@B.com and get his presence information. In order to do so, Alice@A.com may connect directly to B.com and subscribe to Bob's presence information. However, peer network B is not willing to support subscriptions from any user in the network and is willing only to support its users and users that are coming from other peer networks that peer network B trusts.

In reality what will happen is that peer network A will connect to peer network B and will send Alice's subscription on Bob to peer network B. When peer network B has new information on Bob it will send notifications to peer network A that will pass them to Alice.

3.2. List Interdomain Subscription

This is the same as the simple interdomain subscription use case but in this case Alice subscribes to a URI that represents a list of users in peer network B [3]

There are two sub use cases here. One use case is when the list that Alice subscribes to is a list that is configured by e.g. the administrator and it is used to host the names of a group of specifc people e.g. the support group of a company. The other usage is a private group of Alice's friends and the reason that Alice will be using the list instead of doing separate subscriptions is to save on the number of the SUBSCRIBE sessions.

3.3. Authorization Migration

if many users from one peering network watch presentities in another peering network, it may be possible that many watchers from one peering network will subscribe to the same user in the peering network. However, due to privacy constraints, each peering network will have to send multiple copies of the watched presence document. The privacy constraints enable a user to provide different persence document to e.g. friends, co-workers etc. The need to send multiple copies between the peering networks is very inefficient and causes redundant traffic between the peering networks.

In order to make the subscription between peering networks more efficient there needs to be a way to enable peering networks to agree to share privacy information between them. This will enabble sending a single copy (the full copy) of the presence document of of the

watched user and letting the receiving peering network to be responsible to send the right values to the right watchers according to the privacy definitions of the watched user that were delegated to it from the peering network where the watched user resides.

Instead of sharin privacy between the communities, it is also possible to send different copies of the presence document with a list of the watchers that the presence document is intended to. For exeample, if there is a set of watchers in the other community that may see the location of the presentity and another set of users in the other community that may not see the location informaiton, two presence documents will be sent, each one associaed with a list of users that should get it. One presence doucment will contain the location infomrmation and will be associated with a list of users that may see it and the otehr presence document will not contain the location information and will be associated with a list of users that may not see the location information.

3.4. Page mode IM

In this use case a user from one peer network sends a page mode [4] IM to a user on another peer network. As with subscription, the message will pass between the users through the SBEs [2] of the peer networks.

3.5. Session based IM

In this use case a user from one peer network creates an MSRP [5] session with a user from another peer network. The session establishment and the messages will pass between the users through the SBEs [2] of the peer networks.

3.6. Other services

In addition to VOIP sessions which are out of scope for this document only presence and IM are more or less fully standardized. However there are many other services that are being standardized or may be implemented using minimal extensions to existing standards. These include:

- N-way chat - Enable a multi participant chat that will include users from many peer networks.
- File transfer - Send files from a user in one peer network to a user in another peer network.
- Document sharing - Sharing and editing a document between users in different peer networks. Note that document sharing is included

in this document more

There are many more collaboration services that can be thought about. Enabling peering between networks for some of the services will create a basis for defining many more services

3.7. Federation

Federation as defined in [2] is a use case also in real time collaboration.

The none VOIP collaboration features as presence, IM and chat rooms may benefit even more then VOIP services from federation. Collaboration by its definition is something that is stronger where there many more parties collaborating and federation is certainly a good way to achieve greater collaboration.

Additional "side" services as security, lawful interception, logging and more may be provided to the peer networks that are members of the federation.

Note that federation is also known as clearing house in the real time collaboration industry.

4. Security Considerations

This document discusses use cases for peering between communities. It is very clear that the protocols that will enable and make such peering easier will have significant security considerations, there are out of scope for a use case document.

5. Acknowledgments

We would like to thank Jonathan Rosenberg and Roahn Mahy for their input.

6. References

6.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[2] Meyer, D., "SPEERMINT Terminology", draft-ietf-speermint-terminology-06 (work in progress), September 2006.

[3] Roach, A., Campbell, B., and J. Rosenberg, "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", RFC 4662, August 2006.

[4] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[5] Campbell, B., "The Message Session Relay Protocol", draft-ietf-simple-message-sessions-19 (work in progress), February 2007.

Authors' Addresses

Avshalom Houri
IBM
Science Park Building 18/D
Rehovot,
Israel

Email: avshalom@il.ibm.com

Edwin Aoki
AOL LLC
360 W. Caribbean Drive
Sunnyvale, CA 94089
USA

Email: aoki@aol.net

Sriram Parameswar
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Email: Sriram.Parameswar@microsoft.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).