SPEERMINT WG
Internet-Draft
Intended status: Informational
Expires: January 6, 2008

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

July 5, 2007

Presence & Instant Messaging Peering Use Cases
draft-ietf-speermint-consolidated-presence-im-usecases-02.txt

Status of this Memo

Copyright Notice

Abstract

The document describes several use cases of peering of non-VoIP services between two or more Service Providers (SP). These Service Providers create a peering relationship between themselves thus enabling their users to collaborate with users on the other Service Provider network. The target of the document is to drive

requirements for peering between domains that provide the non-VoIP based collaboration services and presence and Instant Messaging (IM) in particular.

Table of Contents

1. Introduction

The document uses the terminology as defined in [2] unless otherwise stated.

Real Time Collaboration (RTC) services become as prevalent and essential for users on the Internet as email. While RTC services can be implemented directly by users in a point-to-point fashion, they are often provided for or on behalf of a Peer Network 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 Peer Network but with those in other Peer Networks as well (similar to the old PSTN that enabled global reachabilty). In practice, each Peer Network is controlled by some domain, and so there is a need to provide for easier establishment of connectivity between Peer Networks, and the management of the relationships between the Peer Networks. This document describes a set of use cases that describe how peering between Peer Networks may be used in non Voice over IP (VoIP) Real Time Collaboration (RTC) services. The use cases are intended to help in identifying and capturing requirements that will guide and then enable a secure and easier peering between Peer Networks that provide non-VoIP RTC services. The use cases for the VoIP RTC services are described in [3].

2. Use Cases

2.1. Simple Interdomain Subscription

Assume two Peer Networks [2], peer network A and peer network B. User Alice@example.com wants to subscribe to user Bob@.example.net and get his presence information. In order to do so, Alice@ domainA.example.com may connect directly to example.net 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.

2.2. List Based Interdomain Subscription

This is similar to the simple interdomain subscription use case except in this case Alice subscribes to a Uniform Resource Identifier (URI) [8] that represents a list of users in peer network B [9] [4]

There are two sub use cases here:

- o The list that Alice subscribes to is a list that is configured by the administrator and it is used to host the names of a group of specific people, e.g. the support group of a company.
- o 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 SUBSCRIBE [6] sessions.

2.3. Authorization Migration

If many users from one Peer Network watch presentities [5] in another Peer Network, it may be possible that many watchers [5] from one Peer Network will subscribe to the same user in the other Peer Network. However, due to privacy constraints, each Peer Network will have to send multiple copies of the watched presence document. The privacy constraints enable a user to provide different presence documents to friends, co-workers etc. The need to send multiple copies between the Peer Networks is very inefficient and causes redundant traffic between the Peer Networks.

In order to make the subscription between Peer Networks more efficient there needs to be a way to enable Peer Networks to agree to share privacy information between them. This will enable sending a single copy (the full copy) of the presence document of the watched user and letting the receiving Peer Network to be responsible to send the right values to the right watchers according to the privacy definitions of the watched users who were delegated to it from the Peer Network where the watched user resides.

Instead of sharing privacy between the Peer Networks, 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 example, if there is a set of watchers in the other Peer Network that may see the location of the presentity and another set of users in the other Peer Network that may not see the location information, two presence documents will be sent, each one associated with a list of users that should receive it. One presence document will contain the location information and will be associated with a list of users that may see it and the other presence document will not contain the location information and will be associated with a list of users that may not see the location information.

2.4. Page Mode IM

In this use case a user from one peer network sends a page mode [7] IM to a user on another peer network. As with subscription, the message will pass between the users through the Signaling path Border

Elements (SBE) [2] of the peer networks.

2.5. Session Based IM

In this use case a user from one peer network creates a Message Session Relay Protocol (MSRP) [10] 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.

2.6. Other Services

In addition to VoIP sessions which are out of scope for this document only presence and IM are nearing standardization completion. In addition to presence and IM, 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 multiple 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: Document sharing is mentioned in this document only for completeness of use cases. It is not standardized by the IETF and will not be included the requirements draft that will result from this document.

The list above is of course not exhaustive as new developments in the world of non-VOIP RTC will surface new services. Enabling peering between networks for some of the services will create a basis for enabling peeering also for future services.

2.7. Federation & Clearing House

Federation as defined in [2] enables peering between multiple Peer Networks. One enablement of a federation can be via a central server that provides services to the Peer Networks or using a peer to peer model that enables many Peer Networks to connect to each other via the peer to peer network. These services can be an N-way chat server, security, lawful interception, logging and more. This type of federation is known also known as a "clearing house".

Non-VoIP services as being usually more text based and consuming less bandwidth may benefit from having a central service that will do central services as logging for them. For example, instead of requiring each Peer- Network to log all messages that are being sent

to the other Peer-Network, this service can be done by the clearing house.

3. IANA Considerations

This document has no actions for IANA.

4. Security Considerations

This document discusses use cases for peering between Peer Networks. It is very clear that the protocols that will enable and make such peering easier will have significant security considerations. The solutions for the security issues is out of scope for this document but here are some examples of security issues that are implied by this document:

When a message is received from a user on another Peer Network, the receiving user, should trust that the other Peer Network have authenticated the user and it is really the user he or she claim to be.
In order to enable peering between big Peer Networks there are some optimizations that will require users of one Peer Network to trust the other Peer Network with respect to their privacy.

5. Acknowledgments

We would like to thank Jonathan Rosenberg, Rohan Mahy, Jason Livingood, Alexander Mayhorfer, Henry Sinnreich and Mohamed Boucadir for their valuable 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] Malas, D. and D. Meyer, "SPEERMINT Terminology", draft-ietf-speermint-terminology-07 (work in progress), June 2007.

[3] Uzelac, A., "VoIP SIP Peering Use Cases",

draft-ietf-speermint-voip-consolidated-usecases-02 (work in progress), June 2007.

[4] Camarillo, G. and A. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)-List Services", draft-ietf-sipping-uri-services-06 (work in progress), September 2006.

[5] Day, M., Rosenberg, J., and H. Sugano, "A Model for Presence and Instant Messaging", RFC 2778, February 2000.

[6] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

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

[8] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

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

[10] 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).