SPEERMINT WG
Internet-Draft
Intended status: Informational
Expires: August 18, 2008

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

February 15, 2008

Presence & Instant Messaging Peering Use Cases
draft-ietf-speermint-consolidated-presence-im-usecases-04.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. 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 [1] 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 Public Switched Telephony Network (PSTN) that enabled global readability). 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) 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 [2].

2. Use Cases

2.1. Simple Interdomain Subscription

Assume two Peer Networks, Peer Network A and Peer Network B. User Alice@example.com (hosted in Peer Network A), wants to subscribe to user Bob@example.net (hosted in Peer Network B) and get his presence information. In order to do so, Alice@example.com could connect directly to example.net and subscribe to Bob's presence information. However, Peer Network B is willing to accept subscriptions and route IMs only when they are coming from its users or 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 to Bob via 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 that in this case Alice subscribes to a Uniform Resource

Identifier (URI) [8] that represents a list of users in Peer Network B [9] [3]

There are several types of lists that Alice may subscribe to:

- Personal group - A list that was created and maintained by Alice and includes Alice's watch list.
- Public group - A list that is created and maintained by an administrator and is typically referred to as a public group. Public groups usually contains a list of specific people that have some common characteristic e.g. support group of a company.
- Ad-hoc group - A list that is short lived and is usually created in a context of some activity that Alice is doing. An ad-hoc group may be created by Alice or by some application. Typical examples may be the list of people that participate with Alice in a conference or a game.

2.3. Authorization Migration

If many users from one Peer Network watch presentities [6] in another Peer Network, it may be possible that many watchers [6] from one Peer Network will subscribe to the same user in the other Peer Network. However, due to privacy constraints that enable a user to provide different presence documents to different watchers, each Peer Network will have to send multiple copies of the watched presence document. 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 for sending the right values to the right watchers according to the delegated privacy policies of the watched users.

Instead of sharing watcher's privacy policies 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 for. 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 is associated with a list of watchers 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.

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.

2.6. Other Services

In addition to VoIP sessions which are out of scope for this document only presence and IM have been ratified as RFCs. 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 textual chat that will include users from multiple Peer Networks. See [4] for more details.
- File transfer - Send files from a user in one Peer Network to a user in another Peer Network. See [5] for more details.
- 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 being 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 peering also for future services.

2.7. Federation & Clearing House

A Federation as defined in [1] enables peering between multiple Peer Networks. A federation may be implemented by means of a central service providing a hub for the Peer Networks or, alternatively, Peer Networks may connect to each other in a peer-to-peer fashion. One of the most important services that this type of federation should provide is authorized interconnection that enables each Peering Network to securely identify other Peering Networks. Other services

that might be provided include an N-way chat server, lawful interception, logging and more. This type of federation is also known as a "Clearing House".

As non-VoIP services are usually text-based and consume less bandwidth, they may benefit from having a central service that will do central services such 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

When Peer Network A peers with Peer Network B, there are several security issues that the administrator of each Peer Network will need mechanisms to verify:

- All communication channels between Peer Network and between each Peer Network and the clearing house have their authenticity and confidentiality protected.
- The other Peer Network is really the Peering Network that it claims to be.
- The other Peer Network is secure and trustful such that information that is passed to it, will not reach a third party. This includes information about specific users as well as information about the authorization policies associated with user information.
- The other Peer Network is secure and trustful such that it will not modify or falsify data that it presents to its users except as required by the authorization policy provided.
- If there is a third party (e.g. a clearing house) involved in the connection between the two Peering Networks that element is also verified to be secure.

The same issues of security are even more important from the point of view of the users of the Peer Networks. Users will have the concern on how their privacy is being adhered to when their presence information is being sent to the other Peer Network. Users today are concerned about providing their email address to a third party when they register to a domain; Presence contains much more sensitive information and the concern of users here will be even deeper.

The privacy issue is even harder if we take into account that in order to enable scalable peering between big Peer Networks there are some optimizations that may require migration of the privacy definitions of users between Peer Network (see Section 2.3). We can imagine the fiasco if a user of one Peer Network will be able to see the privacy information and will learn he/she are listed in a block list of a close friend.

This document discusses use cases for peering between Peer Networks. It is out of scope for the document to provide solutions for security. Nevertheless, it is obvious that the protocols that will enable the use cases that are described here will have to provide for the security considerations described here.

5. Acknowledgments

We would like to thank Jonathan Rosenberg, Jon Peterson, Rohan Mahy, Jason Livingood, Alexander Mayrhofer, Joseph Salowey, Henry Sinnreich and Mohamed Boucadir for their valuable input.

6. Informative References

[1] Malas, D. and D. Meyer, "SPEERMINT Terminology", draft-ietf-speermint-terminology-16 (work in progress), February 2008.

[2] Uzelac, A., "VoIP SIP Peering Use Cases", draft-ietf-speermint-voip-consolidated-usecases-05 (work in progress), February 2008.

[3] 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-07 (work in progress), November 2007.

[4] Niemi, A., Garcia-Martin, M., and G. Sandbakken, "Multi-party Instant Message (IM) Sessions Using the Message Session Relay Protocol (MSRP)", draft-ietf-simple-chat-02 (work in progress), February 2008.

[5] Garcia-Martin, M., Isomaki, M., Camarillo, G., Loreto, S., and P. Kyzivat, "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer", draft-ietf-mmusic-file-transfer-mech-06 (work in progress), December 2007.

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

[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., Mahy, R., and C. Jennings, "The Message Session Relay Protocol (MSRP)", RFC 4975, September 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).