IMSX Protocol Evaluation for Session Based IM

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document is submitted to the SIMPLE WG as part of the ongoing discussion on the selection of the protocol for support of Session Based Instant Messaging. It evaluates the suitability of the IMSX protocol as a transport for Session Based IM. IMSX defines a BEEP profile for exchanging CPIM messages after SIP has performed its session setup signaling. This document evaluates IMSX against the IMPP requirements and its ability to interoperate with other IM systems based upon the CPIM profile.

Table of Contents

1. Overview.................................................................1
   1.1 Background................................................................1
   1.2 IMSX Session Model.................................................2
2. Comparison with IMPP Requirements.................................2
3. Comparison against the CPIM profile...............................5
4. Applicability of IMSX to IM Session Normative Guidelines.....6
5. Conclusions......................................................................8
6. Security Considerations...............................................8
7. References.......................................................................8
1. Overview

1.1 Background

The SIMPLE Working Group bases its requirements on those established by the IMPP Working Group [2] and defines interoperability with other IM protocols with the common message format requirements as defined in CPIM [5]. The Working Group is
Currently evaluating two protocols as a basis for Session Based IM. IM Simple Exchange (IMSX) [3], which defines a profile for using the BEEP protocol [4], is one of the candidates. This document summarizes how well IMSX meets the IMPP requirements. In addition, IMSX is compared against the Abstract Instant Messaging Service as defined by CPIM to see how well it suits the interoperation philosophy. This document also provides some brief discussion on the applicability of IMSX with regards to the Guidelines for Instant Message Sessions [9].

1.2 IMSX Session Model

In the "session" model, an IM application determines that it wishes to communicate with another IM application. These applications, termed the initiating and responding applications (respectively) are conceptually identified using the IM URI, as specified in Section 5.1 of CPIM [5].

The initiating application determines that it will use IMSX to communicate with the responding application, so it uses the SIP URI for this purpose. For example, if the IM application uses IMSX to communicate with an IM application identified as "im:barney@rubble.com", the URI "sip:barney@rubble.com" is utilized for this purpose.

The initiating application ensures that it is running a BEEP entity that implements the IMSX profile, and determines the transport information associated with the BEEP entity (typically IP address and TCP port number). The initiating application then constructs an appropriate SDP to be carried in a SIP INVITE. The initiating application then waits for a response.

The SIP INVITE is received by the responding application, which determines that it wishes to communicate with the initiating application. The responding application ensures that it is running a BEEP entity that implements the IMSX profile. It then determines the transport information associated with the BEEP entity (typically IP address and TCP port number), and sends its own SDP with a 200 response code.

Ultimately, the initiating application receives the response and acknowledges it with a SIP ACK message. Upon receipt of the response, the initiating application activates its BEEP entity, and, using the transport information in the response, establishes a BEEP session. If successful, the initiating application tunes the session as appropriate, and starts the IMSX profile.

2. Comparison with IMPP Requirements
This section contains an evaluation of IMSX against the requirements documented in [2]. \(<x.x.>\) or \(<x.x.x>\) indicates the requirement documented in section \(x.x\) or \(x.x.x\) of [2].

\(<2.1>\) Namespace and Administration

\(<2.1.1>\) The IMSX protocol is entirely independent of whether a PRESENCE SERVICE is available.

\(<2.1.2>\) The IDENTIFIER for reaching the INSTANT INBOX for IMSX does not assume any PRESENTITIES.
<2.1.3> Per <2.1.1.> the IMSX protocol is entirely independent of whether there is a PRESENCE SERVICE, but IMSX does not explicitly preclude the use of the same IDENTIFIER.

<2.1.4> Not Applicable to IM, as ENTITIES are all PRESENCE Related. However, IMSX naming and administration within a DOMAIN is independent of that in any other DOMAIN.

<2.1.5> IMSX/BEEP does not preclude having multiple DOMAINS within a NAMESPACE, thus assuring conformance with this requirement.

<2.2> Scalability

Although all the specific requirements for scalability appear to be applicable only to the PRESENCE SERVICE, due to the use of the term ENTITIES, it is assumed that Scalability should also apply to IM.

IMSX, being based on BEEP, is inherently scalable. Some of the factors contributing to the scalability are:
- BEEP allows for multiple channels over a single session
- The communicating applications are loosely coupled.

<2.3> Access Control

<2.3.5> IMSX controls which other PRINCIPALS can send INSTANT MESSAGES to the INSTANT INBOX by allowing the PRINCIPAL to decline a SIP session being established to send INSTANT MESSAGES. Access control may also be asserted from the IMSX level, by rejecting channel creation or specific messages from other PRINCIPALS.

<2.3.6> IMSX controls which other PRINCIPALS can read INSTANT MESSAGES from that INSTANT INBOX with its support of a secure interface to that INSTANT INBOX. User authentication is achieved using the initial tuning profile. Authorization itself is an internal manner for each BEEP peer. As such, each peer may choose to restrict the operations it allows based on the authentication credentials provided.

<2.3.7> This requirement is specific to the PRESENCE SERVICE, however, it should noted that IM Access control in IMSX is independent of presence.

<2.4> Network Topology

<2.4.3> BEEP is a peer to peer protocol designed to support the sending of the messages directly. However the use of message intermediaries is not precluded.
A solution has been proposed whereby the sender opens a BEEP connection to the first intermediary. The first intermediary connects to the next intermediary (if it exists), and so on. The final intermediary connects to the receiver. Every message sent (either direction) will pass over pre-existing BEEP connections so the TCP setup delay and resources consumption for each hop for each message is avoided.

<2.4.4> Middlebox traversal (NATs and FIREWALLS) for IMSX is a requirement that is currently not specifically addressed by BEEP.
However, it is deemed equivalent to and addressed by the same mechanism which would be used for TCP based SIP media.

<2.5> Message Encryption and Authentication

IMSX defines the means for establishing the level of security through the tuning profile. Although use of the tuning attribute in the SDP announcement is a policy matter, at a minimum, all IMSX implementations must provide the following tuning profiles:

<table>
<thead>
<tr>
<th>tuning value</th>
<th>profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td><a href="http://iana.org/beep/SASL/DIGEST-MD5">http://iana.org/beep/SASL/DIGEST-MD5</a></td>
</tr>
<tr>
<td>integrity</td>
<td><a href="http://iana.org/beep/SASL/DIGEST-MD5">http://iana.org/beep/SASL/DIGEST-MD5</a></td>
</tr>
<tr>
<td>privacy</td>
<td><a href="http://iana.org/beep/TLS">http://iana.org/beep/TLS</a> using the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher and client-side certificates</td>
</tr>
<tr>
<td>all</td>
<td><a href="http://iana.org/beep/TLS">http://iana.org/beep/TLS</a> using the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher and client-side certificates</td>
</tr>
</tbody>
</table>

<2.5.1> IMSX provides a means to ensure confidence that an INSTANT MESSAGE has not been corrupted or tampered with as identified in the table in section <2.5> above. This would be achieved with a tuning value of "integrity" or "all" in the tuning profile.

<2.5.2> IMS provides a means to ensure confidence that a received INSTANT MESSAGE has not been recorded or played back by an adversary as identified in the table in section <2.5> above.

<2.5.3> IMS provides a means to ensure that a sent INSTANT MESSAGE is only readable by ENTITIES that the sender allows with its support of a secure interface. User authentication is achieved using the initial tuning profile. Authorization itself is an internal manner for each BEEP peer. As such, each peer may choose to restrict the operations it allows based on the authentication credentials provided.

<2.5.4> The protocol allows any client to use the means to ensure non-corruption, non-playback, and privacy, but the protocol does NOT require that all clients use these means at all times. IMSX defines the means for establishing the level of security through the tuning profile. Use of the tuning attribute in the SDP announcement is a policy matter, however, at a minimum, all IMSX implementations must provide the following tuning profiles as identified in the table in section <2.5>. The protocol does not require that all clients use these means at all times; the clients
may also turn off these mechanisms using a tuning attribute of "none".

<4.1> Common Message Format

The common message format requirements are met by the definitions defined in CPIM [5]. Evaluation of IMSX against CPIM is described in section 3 of this document.

<4.2> Reliability
<4.2.1> The Response Element defined by IMSX is sent to inform the sender of the INSTANT MESSAGE that the message had been received. The Response contains a Status element that indicates "Success", "Failure", or "Indeterminant". The textual content of the Response is a diagnostic which is meaningful to implementers, perhaps administrators and possibly even end users.

<4.3> Performance

<4.3.1> Once the BEEP session is tuned and the IMSX profile has been exchanged, the processing of the Message and Response elements should provide for a sufficiently rapid exchange of short messages. In addition, the first INSTANT MESSAGE could be piggybacked in the profile exchange up to a limit of 4K octets.

<5.4> Security Requirements related to INSTANT MESSAGES

All the security requirements in section 5.4 of [1] are primarily met by IMSX through the use of TCP and TLS/SASL, unless otherwise specified below. All the requirements identified in this section deal with the scenario where a user A sends an INSTANT MESSAGE M to another user B.

<5.4.1> A MUST receive confirmation of non-delivery

<5.4.2> If M is delivered, B MUST receive the message only once.

<5.4.3> The protocol MUST provide B means of verifying that sent the message.

<5.4.4> B MUST be able to reply to the message via another instant message.

<5.4.5> The protocol MUST NOT always require A to reveal A's IP address, for A to send an instant message. Since, IMSX is based upon the use of SIP for establishing the session, it could be said that IMSX does not meet this requirement as SIP typically reveals the IP Address in several headers including SDP.

<5.4.6> The protocol MUST provide A means of ensuring that no other PRINCIPAL C can see the content of M.

<5.4.7> The protocol MUST provide A means of ensuring that no other PRINCIPAL C can tamper with M, and B means to verify that no tampering has occurred.

<5.4.8> B must be able to read M.

<5.4.9> The protocol MUST allow A to sign the message, using
existing standards for digital signatures.

<5.4.10> B MUST be able to prevent A from sending him messages. For Session based IM, this can be accomplished by B refusing to setup the SIP Session used for IMSX. This may also be handled at the IMSX level by tearing down the channel or the entire session itself.

3. Comparison against the CPIM profile

This section evaluates IMSX against the semantics and data formats defined for CPIM [5]. <x.x.x> or <x.x.x> indicates the requirement
documented in section x.x or x.x.x of CPIM [5]. IMSX has defined its IMSX payload to be conformant to CPIM per the Common Service DTD and Message Service DTD defined in sections 6 and 7 of CPIM [5].

<2.1> Overview of the Messaging Service

IMSX uses its profile and the BEEP message operation 'MSG' to send messages to a peer. IMSX uses its profile and the BEEP response operation 'RPY' to send responses. The transaction identifier is carried in the frame header of the BEEP message.

<2.2> Identification of INSTANT INBOXes

IMSX uses the IM application URI to identify the INSTANT INBOX for a given IM Session as defined in section 5.1 of [1]. This IM application URI is based on the specifications in RFC 2822 [6]. Thus, IMSX should be deemed to be conformant to the specifics necessary for interoperability as identified in <2.2.1> through <2.2.4>. SIP is used to set up the session, thus any required address resolution for Instant Inbox identification may also be performed at session establishment time.

<2.3> Format of Instant Messages

Each BEEP payload exchanged via IMSX consists of an XML document and possibly an arbitrary MIME content. MIME content is included in the BEEP payload by using a "multipart/related" [8], thus IMSX would be compatible with CPIM.

<2.4> The Messaging Service

Section 2.4 of CPIM [5] defines the abstract semantics for the communications between an application and the IM service. In contrast, IMSX is concerned with the semantics for the communications between two IM applications. However, IMSX does define the Message Operation in a manner similar in nature to CPIM's behavior as described in section 2.4.1 of [5]. IMSX does not address the looping of a message through a relay, as described in section 2.4.2 of [5], since its messaging is focused on the exchanges between end-users.

<4> Security Considerations

All the security requirements are met by IMSX primarily through the use of TCP, TLS/SASL. IMSX [3] defines a minimum set of tuning profiles that must be supported as countermeasures to the threats as described in section 4.1 of CPIM [5].
<4.3.1> End-to-end security for Instant Messages

For end-to-end security in section 4.3.1, CPIM suggests MIME-based security (e.g. S/MIME). Although not explicitly specified in BEEP [4] or IMSX [3], IMSX could use S/MIME for the payload.

4. Applicability of IMSX to IM Session Normative Guidelines

This section briefly discusses the applicable of IMSX against the Normative Guidelines described in section 5 of [9].
IMSX satisfies the following guidelines:

- Preliminary signaling used to establish a session of instant messages MUST be capable of negotiating a common underlying transport protocol for instant messaging.

- Session messaging MUST NOT use UDP as a transport layer because of UDP's lack of congestion control. Transport protocols used for session messaging MUST support congestion control.

- A transport/session layer protocol for instant messaging sessions MUST explicitly specify the identities of the participants in the session, a unique session identifier, and sequencing information for messages in a session.

- A transport/session layer solution for instant messaging sessions MUST support end-to-end confidentiality and integrity mechanisms for instant messages.

- A transport/session layer solution for instant messaging sessions MUST support end-to-end mutual authentication.

- A transport/session layer solution for instant messaging sessions SHOULD support a mechanism for specifying a single transport protocol end-to-end.

Although, IMSX/BEEP was not explicitly defined to accommodate network intermediaries, it should be able to satisfy the following guidelines:

- End-to-end security mechanisms for instant messaging sessions SHOULD accommodate network intermediaries that have been authorized to act on the session. For example, headers on which intermediaries need to operate might be kept in cleartext while the remainder of an instant message was encrypted from end-to-end.

- A transport/session layer solution for instant messaging sessions MUST support a mechanism through which a participant in a session can discover the presence of an intermediary. Through the use of the STUN protocol [10], this guideline could be met with the IMSX/BEEP IM Session solution.

IMSX doesn’t meet several of the guidelines with regards to intermediaries, as these guidelines are not in the scope of the BEEP design intent. However, a complete IM Session solution should address the requirements for these guidelines, as they represent
the true operational environment for the IM Session solution:

- Intermediaries SHOULD NOT interpose themselves between endpoints in a session unless they are specifically authorized to do so by one of the principal participants in a session.

- Any intermediaries interposing themselves in instant messaging sessions themselves MUST notify all participants of their presence through either the preliminary signaling or subsequent session messaging.
5. Conclusions

IMSX as defined meets the majority of the CPIM requirements with the exception of the Network topology requirements, defined by <2.4> in section 2, which were beyond the scope of the original design intent of BEEP:

- Middlebox traversal (NATs and FIREWALLS) for IMSX is a requirement that is currently not specifically addressed by BEEP. However, it is deemed equivalent to and addressed by the same mechanism which would be used for TCP based SIP media.

- IMSX does not address the proxy or relay requirements for support of IM. However, as described in section 2 for requirement <2.4.3>, a solution to this requirement is not beyond the scope of BEEP.

Related to these requirements, as evaluated against the IM Session Guidelines in section 4, the IMSX/BEEP IM Session solution does not fully address intermediaries.

Beyond the identified requirements, which are not fully met, additional disadvantages of IMSX as the Session IM protocol are:

- BEEP does not currently support threading.

- Requires the development of a new protocol for most existing SIP products.

There are a few advantages of IMSX that are not necessarily exposed through this detailed evaluation:

- A user can use a single TCP connection for multiple IM Session connections to the same user.

- Several channels may be multiplexed over the same TCP connection having different characteristics.

- For this model of a single TCP connection, interleaving provides a fair share of the use of connection to support the multiple types of media.

6. Security Considerations

Security considerations are addressed by requirements <2.3.> Access Control, <2.5> Message authentication and encryption and <5.4>
Security Requirements related to INSTANT MESSAGES in section 2 of this document and requirements <4> in section 3 of this document.

7. References


Acknowledgements

The author would like to acknowledge the constructive input and feedback given by Sriram Parameswar, which helped to further refine this evaluation.

AuthorÆs Address

Mary Barnes  
Nortel Networks  
2380 Performance Drive  
Richardson, TX USA  
Phone: 1-972-684-5432  
Email: mbarnes@nortelnetworks.com

Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process
must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING 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."