

Message-Id: <200209202101.RAA08202@ietf.org>
To: IETF-Announce: ;
Cc: RFC Editor <rfc-editor@ISI.EDU>, Internet Architecture Board <iab@iab.org>, sip@ietf.org
From: The IESG <iesg-secretary@ietf.org>
Subject: Protocol Action: Session Initiation Protocol Extension for Instant Messaging to Proposed Standard
Date: Fri, 20 Sep 2002 17:01:32 -0400
Sender: scoya@cnri.reston.va.us

The IESG has approved the Internet-Draft 'Session Initiation Protocol Extension for Instant Messaging' <draft-ietf-sip-message-07.txt> as a Proposed Standard. This document is the product of the Session Initiation Protocol Working Group. The IESG contact persons are Allison Mankin and Scott Bradner.

Technical Summary

RFC 2778 and RFC 2779 give a model and requirements for presence and instant messaging protocols. The Session Initiation Protocol (RFC 3261) provides mechanisms that are useful for presence applications, and for session-oriented communication applications. This document specifies a new method for SIP called MESSAGE, which adds an instant message mechanism as well, fulfilling RFC 2779. This IM mechanism is intended for pager style use, in which a MESSAGE carries a short text, or message/cpim body, as a stand-alone communication, rather than a stream of connected data, in a "session mode." The SIMPLE working group is currently working to understand the session model more fully and determine how SIMPLE should best support it (for instance with multiple types of session modes).

Working Group Summary

The requirements for this specification originated in the IMPP and SIMPLE Working Groups, and then the protocol extension was completed by SIP. The major point of contention was to ensure that MESSAGE did not become a congestion-prone transport-replacement, taking advantage of SIP's original ability to run over UDP. Fortunately, beginning with RFC 3261, any SIP message with a large payload is likely to use TCP for its transport. The MESSAGE specification achieved strong working group and Transport area consensus after vigorous discussion of its first few revisions.

Protocol Quality

Allison Mankin reviewed the specification for the IESG.
Several early commercial implementations have been identified.

Note to RFC Editor:

Please make the following changes:

Before the Introduction, add an unnumbered section -

Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 and indicate requirement levels for compliant SIP implementations.

References

Add RFC 2119 to Normative references.

11. Security Considerations

Old:

In particular, UAs that support the MESSAGE request SHOULD support end-to-end authentication, body integrity, and body confidentiality mechanisms.

New:

In particular, UAs that support the MESSAGE request MUST implement end-to-end authentication, body integrity, and body confidentiality mechanisms.

11.1 Outbound authentication

Old:

When local proxies are used for transmission of outbound messages, proxy authentication is RECOMMENDED. This is useful to verify the identity of the originator, and prevent spoofing and spamming at the originating network.

New:

When local proxies are used for transmission of outbound messages, proxy authentication, as specified in RFC 3261, is RECOMMENDED. This is useful to verify the identity of the originator, and prevent spoofing and spamming at the originating network.

11.3 End-to-End Protection

Old:

To alleviate the concerns stated above, the MESSAGE bodies SHOULD be secured with S/MIME.

New:

For remedying the concerns stated above, the MESSAGE bodies MUST be secured with S/MIME. If bodies specified in future to be carried by the MESSAGE method have different means of providing end-to-end security, their specification MUST describe the usage.

11.4 Replay Prevention

OLD:

To prevent the replay of old SIP requests, all signed MESSAGE requests and responses SHOULD contain a Date header field covered by the message signature.

NEW:

To prevent the replay of old SIP requests, all signed MESSAGE requests and responses MUST contain a Date header field covered by the message signature.