

SIP
Internet-Draft
Expires: June 26, 2003

J. Rosenberg
dynamicsoft
December 26, 2002

**The Session Initiation Protocol (SIP) INFO Method Considered Harmful
draft-rosenberg-sip-info-harmful-00**

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>.

This Internet-Draft will expire on June 26, 2003.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

The Session Initiation Protocol (SIP) INFO method defines a means for transporting mid-dialog application layer data between user agents. Its initial use was to support the transport of ISUP mid-call messages which could not be mapped to any other SIP request method. However, since its initial usage for that purpose, INFO has seen widespread abuse as a means for introducing non-standard and non-interoperable extensions to SIP. For this reason, we now believe INFO should be considered harmful, and therefore, deprecated in its current form.

Table of Contents

1.	Introduction	3
2.	Problems with INFO	4
3.	Proposed Solution	6
4.	Security Considerations	7
5.	Acknowledgments	8
	Informative References	9
	Author's Address	9
	Intellectual Property and Copyright Statements	10

1. Introduction

The Session Initiation Protocol (SIP), was first published as [RFC 2543](#) [2] in March of 1999, and later revised as [RFC 3261](#) [1] in June 2002. SIP was engineered to support extensions, through new methods, new headers, new parameters, and new body types. The first extension to SIP that was published after [RFC 2543](#) (and indeed, the only one published before SIP itself was revised), was the SIP INFO method, documented in [RFC 2976](#) [3].

The original application of the INFO method was to support the transport of ISUP mid-call signaling messages, as part of the SIP-T [6] framework. However, the group believed that transport of ISUP messages was an overly narrow problem space. So, the scope of the INFO method was expanded to allow for the transport of any application layer mid-call signaling. As long as it didn't modify the dialog or transaction state, it was a legal usage of INFO.

Unfortunately, since the publication of [RFC 2976](#), there has been extensive misuse of INFO to support vendor proprietary extensions, resulting in loss of interoperability, amongst other things. [Section 2](#) overviews the problems with the current specification, and [Section 3](#) proposes a path forward.

2. Problems with INFO

The problems with INFO derive from its lack of any well defined semantic. [Section 2](#), which overviews the INFO method, has this to say:

There are no specific semantics associated with INFO. The semantics are derived from the body or new headers defined for usage in INFO.

This means that INFO is purposefully defined as a tunneling protocol for other extensions. Indeed, it has been proposed (and in fact, used), for a wide variety of functions, including:

- o The transport of DTMF digits to proxies and user agents
- o Control of media servers
- o Control of video encoding (fast intra updates, picture freeze)[[9](#)]
- o Managing QoS reservations [[8](#)]
- o Floor control

There are several problems with these usages:

Lack of Interoperability. None of these usages interoperate. Part of the problem is that many are vendor extensions which are not described through any IETF specifications. Another problem is that INFO itself provides no way to signal the actual usage. Interoperation depends on configuration to properly determine the implied INFO usage.

Inappropriateness. Many of these usages are not proper usages for SIP. The guidelines for authors of SIP extensions [[7](#)] clearly rules some of them, such as media server control, out of scope. Since INFO is effectively a way to tunnel information between two endpoints connected through SIP, it appears to attract any kind of usage that requires bidirectional information transfer. Many such usages are inappropriate because of the scaling issues (proxy overload), timing issues, and sequencing issues that arise when SIP is used.

Incorrectness. Many of these extensions and usages have protocol errors, security weaknesses, race conditions, and so on. These are typically the result of insufficient review by the working group. Such reviews never take place because the INFO method does not define any framework by which its usages can be defined. It

does not specify any means by which vendors can publish informational usages, and thereby obtain IETF review.

It is our belief that the root cause of these troubles is that INFO is a "content-free framework". It is a framework because it leaves actual protocol semantics to usages - other extensions - which ride ontop of INFO. Its goal as a framework is to support mid-call information transfer unrelated to SIP dialog or transaction state. However, it is "content-free" because it doesn't describe any means by which those extensions can be used in an interoperable way. This is in contrast to the SIP events framework [\[4\]](#), which defines a way to specify packages that build on the framework. It defines an IANA registration procedure, describes guidelines for when the SIP events framework should be used, specifies framework-specific behaviors, and specifies a means for indicating support for particular packages. We believe all of these features are essential for any protocol that defines itself as a framework.

However, none of these features are defined in [RFC 2976](#). There are no IANA procedures for "INFO extensions", no guidelines for what makes a good INFO usage, and no means of indicating support for a particular INFO usage. Perhaps most interestingly, it does not specify any semantics for INFO itself. Nothing about INFO processing differs from any other method. Any new feature could be defined using a new method, and would suffer no duplication of functionality compared to defining it as a new usage of INFO. It is this latter characteristic which truly makes it content-free. What is the value of a framework that provides no semantics whatsoever? There is no value.

3. Proposed Solution

There are a few directions that can be taken to remedy this problem. We enumerate them all for completeness:

1. Do nothing.
2. Revise [RFC 2976](#), turning it into a proper framework. That would mean the specification of an IANA registration procedure, usage guidelines, and so on, patterned after [RFC 3265](#).
3. Revise [RFC 2976](#), restricting its usage to the only approved one - support for SIP-T.

We believe that the proper course of action is the third. While the second of these seems attractive, there is really little value. That's because INFO does not actually define any semantics. The SIP events framework, by contrast, defines a significant amount of behavior as part of the framework. Indeed, one might argue that the vast majority of the semantics of any package exist in the framework. It is merely the definition of some defaults, and the establishment of some guidelines, which rest purely with the package. The exact opposite is true of INFO. In fact, it is not clear that there are any general, usage independent semantics that could be defined. In the absence of such semantics, the usage of a framework provides no value.

Option 3 would allow us to retain backwards compatibility with the only approved usage (and one of the most common ones). Any other usage would be non-standard. The functions that were previously being provided by INFO usages would now need to be specified as proper SIP extensions, and would therefore be subject to the SIP change process [5]. That will be valuable in addressing many of the problems outlined in [Section 2](#). The SIP change process will ensure that the extension is a proper SIP usage, is correct in its behavior, and that it interoperates.

4. Security Considerations

Well documented and reviewed protocols always provide better security than hacks piled ontop of a vague framework. Therefore, we believe this proposal will generally improve the security of the Internet.

5. Acknowledgments

Credit goes to Dean Willis for suggesting, at some point, that INFO could be reformulated as a framework along the lines of [RFC 3265](#). It is also worth mentioning that the faults of [RFC 2976](#) do not lie with its author, who is a respected contributor in the SIP community. At the time of publication, it represented our best understanding of the way to approach the problem. Significant experience has been gained since its publication, and it is that experience which has led us to conclude that the direction was ultimately not the right one.

Informative References

- [1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), June 2002.
- [2] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", [RFC 2543](#), March 1999.
- [3] Donovan, S., "The SIP INFO Method", [RFC 2976](#), October 2000.
- [4] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", [RFC 3265](#), June 2002.
- [5] Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J. and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)", [BCP 67](#), [RFC 3427](#), December 2002.
- [6] Vemuri, A. and J. Peterson, "Session Initiation Protocol for Telephones (SIP-T): (SIP-T): Context and Architectures", [BCP 63](#), [RFC 3372](#), September 2002.
- [7] Rosenberg, J., "Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)", [draft-ietf-sip-guidelines-06](#) (work in progress), November 2002.
- [8] Salsano, S., Veltri, L. and D. Papalilo, "SIP Extensions for QoS support", [draft-veltri-sip-qsip-01](#) (work in progress), October 2002.
- [9] Levin, O., Olson, S. and R. Even, "XML Schema for Media Control", [draft-levin-mmusic-xml-media-control-00](#) (work in progress), October 2002.

Author's Address

Jonathan Rosenberg
dynamicsoft
72 Eagle Rock Avenue
East Hanover, NJ 07936
US

Phone: +1 973 952-5000
EMail: jdrosen@dynamicsoft.com
URI: <http://www.jdrosen.net>

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

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 assignees.

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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the
Internet Society.