Requirements and Framework for Session Initiation Protocol (SIP) Exploder Invocation
draft-camarillo-sipping-exploders-03.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

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 August 1, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document describes the need for SIP exploders and provides requirements for their invocation. Additionally, it defines a framework which includes all the SIP extensions needed to meet these requirements.
Table of Contents

1. Introduction ................................................. 3
2. Terminology ............................................... 3
3. Requirements ............................................... 3
4. Framework .................................................. 4
   4.1 Carrying URI Lists in SIP ............................. 4
   4.2 Exploder Processing of URI Lists ..................... 4
   4.3 Explosion's Results ..................................... 5
5. Security Considerations ................................. 5
6. Acknowledges ............................................... 6
7. References ................................................. 6
   7.1 Normative References ................................. 6
   7.2 Informational References .............................. 7
    Author's Address ......................................... 7
    Intellectual Property and Copyright Statements ....... 8
1. Introduction

Some applications require that, at a given moment, a SIP [2] UA (User Agent) performs a similar transaction with a number of remote UAs. For example, an instant messaging application that needs to send a particular message (e.g., "Hello folks") to n receivers needs to send n MESSAGE requests; one to each receiver.

When the transaction that needs to be repeated consists of a large request, or the number of recipients is high, or both, the access network of the UA needs to carry a considerable amount of traffic. Completing all the transactions on a low-bandwidth access would require a long time. This is unacceptable for a number of applications.

A solution to this problem consists of introducing exploders in the network. The task of an exploder is to receive a request from a UA and send a number of similar requests to a number of destinations. Once the requests are sent, the exploder typically informs the UA about their status. Effectively, the exploder behaves as a B2BUA (Back-To-Back-User-Agent).

Note that resource lists, as described in [4], already use SIP exploders for SUBSCRIBE transactions. Still, the set of destinations needs to be preconfigured using out-of-band mechanisms (e.g., XCAP).

The Advanced Instant Messaging Requirements for SIP [5] also mentions the need for exploders for MESSAGE transactions:

"REQ-GROUP-3: It MUST be possible for a user to send to an ad-hoc group, where the identities of the recipients are carried in the message itself."

The remainder of this document provides requirements to invoke exploders in an efficient manner and a framework that meets these requirements.

2. 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 [1] and indicate requirement levels for compliant implementations.

3. Requirements

This section contains the requirements:
1. The invocation mechanism MUST allow the invoker to provide a list of destination URIs to the exploder. This URI list MAY consist of one or more URIs.
2. The mechanism to provide the URI list to the exploder MUST NOT be request specific.
3. The invocation mechanism SHOULD NOT require more than one RTT (Round-Trip Time).
4. An exploder MAY provide services beyond request explosion. That is, exploders can be modelled as application servers. For example, an exploder handling INVITE requests may behave as a conference server and perform media mixing for all the participants.
5. The interpretation of the meaning of the URI list sent by the invoker MUST be at the discretion of the application to which the list is sent.
6. It MUST be possible for the invoker to find out about the result of the operations performed by the application server with the URI list. An invoker may, for instance, be interested in the status of the transactions initiated by the exploder.
7. Exploders MUST NOT perform any request explosion without authenticating the invoker.

4. Framework

Although Section 3 contains specific requirements for SIP exploders, this framework is not restricted to application servers that only provide request explosion services. Per requirement number 4, we also deal with application servers that provide a particular service that includes a request explosion (e.g., a conference server that INVITEs several participants which are chosen by a user agent).

4.1 Carrying URI Lists in SIP

Requirements 1 through 3 indentify the need for a request-independent mechanism to provide a SIP exploder with a URI list in a single RTT. The mechanism described in [3] meets these three requirements.

UAs (User Agents) add a "list" SIP and SIPS URI parameter to the Request-URI of the request. This "list" parameter points to a body part which contains the URI list. The default URI list format for SIP entities is the XCAP resource list format defined in [6].

4.2 Exploder Processing of URI Lists

According to Requirement 4 and 5, exploders can behave as application servers. That is, taking a URI list as an input, they can provide arbitrary services.
So, the interpretation of the URI list by the server depends on the service to be provided. For example, for a conference server, the URIs in the list may identify the initial set of participants. On the other hand, for a MESSAGE exploder, the URIs in the list may identify the recipients of an instant message.

At the SIP level, this implies that the behavior of application servers receiving requests with URI lists SHOULD be specified on a per method basis. Examples of such specifications are [draft-camarillo-sipping-adhoc-conferencing-00.txt] for INVITE, [draft-garcia-sipping-message-exploder-00.txt] for MESSAGE, and [draft-camarillo-sipping-adhoc-simple-00.txt] for SUBSCRIBE.

### 4.3 Explosion's Results

According to requirement 6, user agents should have a way to obtain information about the operations performed by the application server. Since these operations are service specific, the way user agents are kept informed is also service specific. For example, a user agent establishing an adhoc conference with an INVITE with a URI list may discover which participants were successfully brought in into the conference by using the conference package [8].

### 5. Security Considerations

Security plays an important role in the implementation of any exploder. By definition, and exploder takes one request in and sends a potentially large number of them out. Attackers may attempt to use exploders as traffic amplifiers to launch DoS attacks. In addition, malicious users may attempt to use exploders to distribute unsolicited messages (i.e., SPAM) or to make unsolicited VoIP calls. This section provides guidelines to avoid these attacks.

Exploders MUST NOT perform any request explosion for an unauthorized user. So, exploders MUST authenticate users and check whether they are authorized to request the exploder's services before performing any request explosion.

Even though the previous rule keeps unauthorized users from using exploders, authorized users may still launch attacks using a exploder. If an exploder is used to send unsolicited requests to one or several destinations, it should be possible to track down the sender of such requests. To do that, exploders MAY provide information about the identity of the original sender of the request in their outgoing requests. Exploders can use Authenticated Identity Bodies (AIB) [7] or P-Asserted-Identity header fields [9] to provide this information. Furthermore, it is RECOMMENDED that exploders keep a log of all the transactions they handle (for a reasonable period of
time), so that SPAMMERS can be tracked down.

The previous rule allows exploders to track down attackers once an attack has taken place. Nevertheless, it is often desirable to prevent the attack in the first place, instead of taking measures afterwards. Providing the identify of the original sender in outgoing requests is not enough to prevent attacks because victims may consist of non-SIP nodes which would not be able to decline SIP requests using SIP error responses.

Exploders MUST NOT explode a request to a destination which has not agreed to receive requests from the exploder beforehand. Users can agree to receive requests from an exploder in several ways, such as filling a web page, sending an email, or signing a contract. Additionally, users MUST be able to further describe the explosions they are willing to receive. For example, a user may only want to receive explosions performed by a particular exploder on behalf of a particular user. Effectively, these rules make URI lists used by exploders opt-in.

Exploders MAY have policies that limit the number of URIs in the list, as a very long list could be used in a denial of service attack to place a large burden on the exploder to send a large number of SIP requests.

Requirement 7, which states that exploders need to authenticate requesters of request explosions, and the previous rules apply to exploders in general. In addition, specifications dealing with individual methods MUST describe the security issues that relate to each particular method.

6. Acknowledges

Duncan Mills and Miguel A. Garcia-Martin supported the idea of 1 to n MESSAGEs. Jon Peterson provided useful comments.

7. References

7.1 Normative References


7.2 Informational References


Author's Address

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com