Network Working Group
Request for Comments: 5318
Category: Informational

J. Hautakorpi
G. Camarillo
Ericsson

December 2008

The Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header)

Status of This Memo

Copyright Notice

Abstract

This document specifies the Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header). This P-Header is used in the Open Mobile Alliance's (OMA) Push to talk over Cellular (PoC) system. It enables URI-list servers to refuse the handling of incoming URI lists that have embedded URI lists. This P-Header also makes it possible for the URI-list server to inform the client about the embedded URI list that caused the rejection and the individual URIs that form such a URI list.

Table of Contents

1. Introduction

The Open Mobile Alliance (OMA) has specified the Push to talk over Cellular (PoC) service, which uses the Session Initiation Protocol (SIP) [3] and Uniform Resource Identifier (URI)-list services [5] (more information about OMA PoC can be found at [8]).

OMA PoC needs a mechanism for servers to refuse the handling of incoming URI lists when these have embedded URI lists. Such a mechanism is intended to be used to establish a particular type of PoC session called an ad-hoc PoC group session.

The remainder of this document is organized as follows. Section 3 describes the scenario where the mechanism will be used. Section 4 provides an overview of the mechanism, which includes a new P-Header called P-Refused-URI-List. Section 5 defines the syntax of this new P-Header. Section 6 specifies how to use the P-Header. Section 7 provides a usage example. Section 8 describes the applicability of the P-Header. Security considerations are discussed in Section 9 and, finally, the IANA considerations are stated in Section 10.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

3. Usage Scenario

An ad-hoc PoC group session is a type of multi-party PoC session. The originator of a particular ad-hoc PoC group session chooses in an ad-hoc manner (e.g., selecting from an address book) the set of desired participants. In order to establish the ad-hoc PoC group session, the originator sends an INVITE request with a URI list that contains the URIs of those participants.

The PoC network, following the procedures defined in [6], receives such an INVITE request and generates an individual INVITE request towards each of the URIs in the URI list.

In previous versions of the OMA PoC service, the originator of an ad-hoc PoC group session was only allowed to populate the initial URI list with URIs identifying individual PoC users. Later versions of the service allow the originator to also include URI lists whose entries represent URI lists. That is, the initial URI list contains entries that are URI lists themselves. The expected service behavior then is that the members of the embedded URI lists are invited to join the ad-hoc PoC group session.

Figure 1 illustrates the desired behavior. The originator (not shown) places the URI list friends@example.org, along with the URI alice@example.com, in the initial URI list. The PoC network resolves friends@example.org into its members, bob@example.org and carol@example.net, and sends INVITE requests to all the recipients.

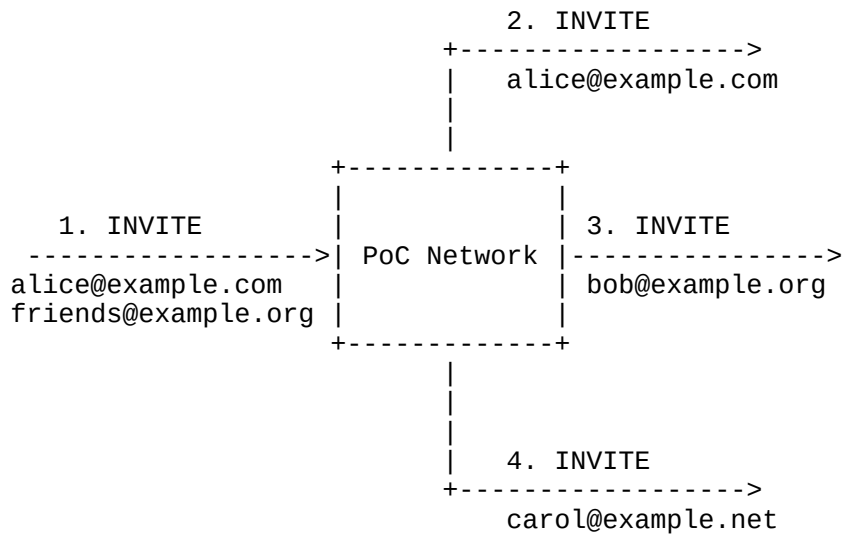

Figure 1: PoC Expected Behavior

The PoC network in Figure 1 consists of PoC servers, which are SIP entities that can behave as proxies or B2BUAs (Back-to-Back User Agents). There are two types of logical PoC servers: controlling and participating.

In an ad-hoc PoC group session, there is always exactly one controlling PoC server. The controlling PoC server of an ad-hoc PoC group session resolves an incoming URI list and sends INVITEs to the members of the list. The controlling PoC server also functions as the focus of the session. Every participant in an ad-hoc PoC group has an associated participating PoC server, which resides in the home domain of the participant.

Figure 2 shows how the PoC servers of the PoC network behave in the scenario shown in Figure 1. An originating PoC user agent sends an INVITE request (1) with a URI list to its participating PoC server. The participating PoC server of the originator receives the INVITE request, assumes the role of controlling PoC server for the ad-hoc PoC group session, and sends an INVITE request to each of the URIs in the URI list.

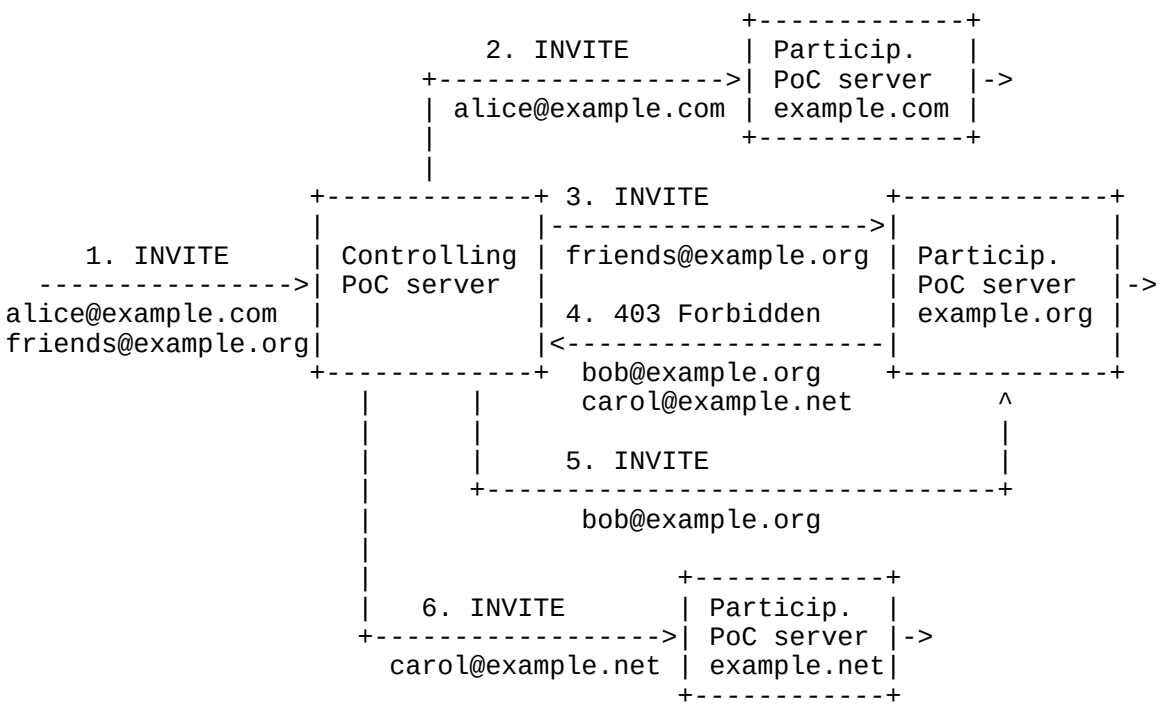

Figure 2: PoC Network Behavior

The first URI of the list, alice@example.com, identifies a single user. The second URI of the URI list, friends@example.org, identifies a URI list. In PoC terminology, friends@example.com identifies a pre-arranged PoC group. The PoC server at example.org, which knows the membership of friends@example.com, cannot send INVITE requests to the members of friends@example.org because that PoC server does not act as a controlling PoC server for the ad-hoc PoC group session being established. Instead, it informs the controlling PoC server that friends@example.org is a list whose members are bob@example.org and carol@example.net. Upon receiving this information, the controlling PoC server generates INVITE requests towards bob@example.org and carol@example.net.

Although not shown in the above example, the participating PoC server (example.org) can include -- based on policy, presence of the members, etc. -- just a partial list of URIs of the URI list. Furthermore, a URI that the participating PoC server returns can be a URI list.

At present, there is not a mechanism for a participating PoC server to inform a controlling PoC server that a URI identifies a list and the members of that list, nor is there a mechanism to indicate the URIs contained in the list. This document defines such a mechanism: the P-Refused-URI-List P-Header.

4. Overview of Operation

When a URI-list server receives an INVITE request with a URI list containing entries that are URI lists themselves, and the server cannot handle the request, it returns a 403 (Forbidden) response with a P-Refused-URI-List P-Header, as shown in Figure 3. The P-Refused-URI-List P-Header contains the members of the URI list or lists that caused the rejection of the request. This way, the client can send requests directly to those member URIs.

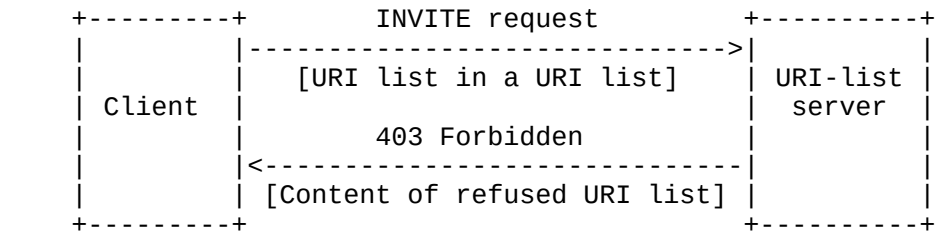

Figure 3: Operational Overview

5. Syntax of P-Refused-URI-List Header Field

The following is the augmented Backus-Naur Form (BNF) [4] syntax of the P-Refused-URI-List P-Header:

```
P-Refused-URI-List = "P-Refused-URI-List" HCOLON
                          uri-list-entry
                          *(COMMA uri-list-entry)
uri-list-entry     = ( name-addr / addr-spec )
                          *( SEMI refused-param )
refused-param      = members-param / generic-param
members-param      = "members" EQUAL
                          LDQUOT *( qdtext / quoted-pair ) RDQUOT
```

The members P-Header parameter MUST contain a cid-url, which is defined in RFC 2392 [2].

The HCOLON, SEMI, EQUAL, LDQUOT, RDQUOT, and generic-param are defined in [3].

6. Response Generation

A 403 (Forbidden) response can contain more than one P-Refused-URI-List entries. The P-Refused-URI-List header field MUST NOT be used with any other response. The P-Refused-URI-List P-Header contains one or more URIs, which were present in the URI list in the incoming request and could not be handled by the server. Additionally, the P-Refused-URI-List can optionally carry some or all of the members of the URI lists identified by those URIs.

The 403 (Forbidden) response MAY contain body parts which contain URI lists. Those body parts can be referenced by the P-Refused-URI-List entries through their Content-IDs [2]. If there is a Content-ID defined in the P-Refused-URI-List, one of the body parts MUST have an equivalent Content-ID. The format of a URI list is service specific.

This kind of message structure enables clients to determine which URI relates to which URI list, if the URI-list server is willing to disclose that information. Furthermore, the information enclosed in the URI lists enable clients to take further actions to remedy the rejection situation (e.g., send individual requests to the members of the URI list).

7. Message Sequence Example

In the following message sequence example, a controlling PoC server sends an INVITE request to a participating PoC server. The participating PoC server rejects the request with a 403 (Forbidden) response. The 403 response has a P-Refused-URI-List P-Header that carries the members of the rejected URI lists that the participating PoC server determines to disclose to this controlling PoC server in the body of the message.

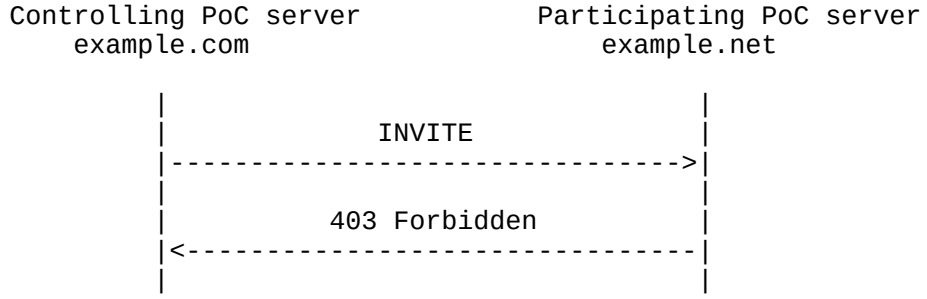

Figure 4: Message Sequence Example

The INVITE request shown in Figure 4 is as follows (Via header fields are not shown for simplicity):

```
INVITE sip:poc-service@example.net SIP/2.0
Max-Forwards: 70
From: PoC service <sip:poc-service@example.com>;tag=4fxaed73sl
To: PoC service <sip:poc-service@example.net>
Call-ID: 7xTn9vxNit65XU7p4@example.com
CSeq: 1 INVITE
Contact: <sip:poc-service@poc-as.example.com>
Require: recipient-list-invite
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: 538

--boundary1
Content-Type: application/sdp

(SDP not shown)

--boundary1
Content-Type: application/resource-lists+xml
Content-Disposition: recipient-list

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists">
  <list>
    <entry uri="sip:bob@example.net"/>
    <entry uri="sip:friends-list@example.net"/>
    <entry uri="sip:colleagues-list@example.net"/>
  </list>
</resource-lists>
--boundary1--
```

The URIs sip:friends-list@example.net and sip:colleagues-list@example.net in the example above are actually references to URI lists (i.e., pre-arranged PoC groups). In the following response, the URI lists are in the XML resource list format [7].

The content of the 403 (Forbidden) response in Figure 4 is as follows (Via header fields are not shown for simplicity):

```
SIP/2.0 403 Forbidden
From: PoC service <sip:poc-service@example.com>;tag=4fxaed73sl
To: PoC service <sip:poc-service@example.net>;tag=814254
Call-ID: 7xTn9vxNit65XU7p4@example.com
CSeq: 1 INVITE
P-Refused-URI-List: sip:friends-list@example.net;
  members=<cid:an3bt8jf03@example.net>
P-Refused-URI-List: sip:colleagues-list@example.net;
```

```
  members=<cid:bn35n8jf04@example.net>
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: 745

--boundary1
Content-Type: application/resource-lists+xml
Content-Disposition: recipient-list
Content-ID: <an3bt8jf03@example.net>

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists">
  <list>
    <entry uri="sip:bill@example.org"/>
    <entry uri="sip:randy@example.com"/>
    <entry uri="sip:eddy@example.com"/>
  </list>
</resource-lists>

--boundary1
Content-Type: application/resource-lists+xml
Content-Disposition: recipient-list
Content-ID: <bn35n8jf04@example.net>

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists">
  <list>
    <entry uri="sip:joe@example.org"/>
    <entry uri="sip:carol@example.com"/>
  </list>
</resource-lists>
--boundary1--
```

Using the message body of the 403 (Forbidden) response above, the controlling PoC server can determine the members of sip:friend-list@example.net and sip:colleagues-list@example.net that the participating PoC server determines to disclose to this controlling PoC server. Furthermore, the controlling PoC server can deduce that the participating PoC server has not sent any outgoing requests, per regular URI-list server procedures.

8. Applicability

The P-Refused-URI-List header field is intended to be used in OMA PoC networks. This header field is used between PoC servers and carries information about those URI lists that were rejected by the server receiving the request.

The OMA PoC services is designed so that, in a given session, only one PoC server can resolve incoming URI lists and send INVITEs to members of these lists. This restriction is not present on services developed to be used on the public Internet. Therefore, the P-Refused-URI-List P-Header does not seem to have general applicability outside the OMA PoC service.

Additionally, the use of the P-Refused-URI-List P-Header requires special trust relationships between servers that do not typically exist on the public Internet.

It is important to note that the P-Refused-URI-List is optional and does not change the basic behavior of a SIP URI-list service. The P-Refused-URI-List only provides clients with additional information about the refusal of the request.

9. Security Considerations

It is assumed that the network elements handling the P-Refused-URI-List P-Header are trusted. Also, attackers are not supposed to have access to the protocol messages between those elements. This is because the P-Refused-URI-List is intended to be used in the OMA PoC environment, which is implemented in the operators' core network; for more on OMA PoC security assumptions, see [9]. Traffic protection between network elements is achieved by using IP Security (IPsec) and sometimes by physically protecting the network.

However, implementors and administrators should be aware of two special security considerations related to the use of P-Refused-URI-List:

Eavesdropping: 403 (Forbidden) responses may contain information about the members of a given URI list. Eavesdroppers can acquire this information if the 403 (Forbidden) responses are not encrypted. Therefore, it is RECOMMENDED that either hop-by-hop or end-to-end encryption (e.g., using TLS or S/MIME, respectively) is used.

Disclosing information: A rogue entity may be able to acquire information about the members of a given URI list if the URI-list server sends information about those URI lists to unauthorized users. Therefore, it is RECOMMENDED that a URI-list server discloses the content of that URI-list only to authorized clients.

10. IANA Considerations

The IANA has made two additions to the Session Initiation Protocol (SIP) Parameters registry. The following header field has been added to the Header Fields sub-registry.

Header Name	compact	Reference
P-Refused-URI-List		[RFC5318]

The following header field parameter has been added to the Header Field Parameters and Parameter Values sub-registry.

Header Field	Parameter Name	Predefined Values	Reference
P-Refused-URI-List	members	No	[RFC5318]

11. Acknowledgements

Authors would like to thank Tom Hiller who did a thorough, dedicated review for this document.

12. References

12.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", RFC 2392, August 1998.

[3] 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.

[4] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[5] Camarillo, G. and A. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) URI-List Services", RFC 5363, October 2008.

[6] Camarillo, G. and A. Johnston, "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)", RFC 5366, October 2008.

12.2. Informative References

[7] Rosenberg, J., "Extensible Markup Language (XML) Formats for Representing Resource Lists", RFC 4826, May 2007.

[8] Open Mobile Alliance, "OMA PoC System Description: Draft Version 2.0", April 2007.

[9] Open Mobile Alliance, "Push to talk over Cellular (PoC) - Architecture: Draft Version 2.0", April 2007.

Authors' Addresses

Jani Hautakorpi
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Jani.Hautakorpi@ericsson.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com