Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: November 16, 2017

P. Dawes
Vodafone Group
C. Arunachalam
Cisco Systems

May 15, 2017

Marking SIP Messages to be Logged
draft-ietf-insipid-logme-marking-07

Abstract

SIP networks use signaling monitoring tools to diagnose user reported problems and for regression testing if network or user agent software is upgraded. As networks grow and become interconnected, including connection via transit networks, it becomes impractical to predict the path that SIP signaling will take between user agents, and therefore impractical to monitor SIP signaling end-to-end.

This document describes an indicator for the SIP protocol which can be used to mark signaling as of interest to logging. Such marking will typically be applied as part of network testing controlled by the network operator and not used in regular user agent signaling. However, such marking can be carried end-to-end including the originating and terminating SIP user agents, even if a session originates and terminates in different networks.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

When users experience problems with setting up sessions using SIP, enterprise or service provider network operators need to identify root cause by examining the SIP signaling. Also, when network or user agent software or hardware is upgraded regression testing is needed. Such diagnostics apply to a small proportion of network traffic and can apply end-to-end, even if signaling crosses several networks possibly belonging to several different network operators. It may not be possible to predict the path through those networks in advance, therefore a mechanism is needed to mark a session as being of interest so that SIP entities along the signaling path can provide diagnostic logging. [RFC8123] illustrates this motivating scenario. This document describes a solution that meets the requirements for such 'log me' marking of SIP signaling also defined in [RFC8123].

This document defines a new header field parameter "logme" for the "Session-ID" header field. Implementations of this document MUST implement session identity specified in [RFC7989].

2. Requirements Language

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 [RFC2119], except that rather than describing interoperability requirements, they are used to describe requirements to be satisfied by the "log me" marking solution.

3. "Log Me" Marking Protocol Aspects

3.1. Session-ID logme Parameter

Logging is most effective when it is applied end-to-end for a communication session. This ability requires "log me" marker to be passed through SIP intermediaries. Session-ID header defined in ([RFC7989]) was chosen to carry the "log me" marker as a "logme" parameter since the session identifier is passed through SIP B2BUAs or other intermediaries. The "logme" parameter shown in Figure 1 does not introduce any device-specific or user-specific information and MUST be passed unchanged through SIP B2BUAs or other intermediaries.

```
        Alice           Proxy           Registrar
        u1.foocorp.com  p1.foocorp.com  r1.foocorp.com
        |                  |                  |
        |(1) INVITE        |                  |
        | Session-ID: ab30317f1a784dc48ff824d0d3715d86;
        |  remote=47755a9de7794ba387653f2099600ef2;logme
        |----------------->|                  |
        |                  |                  |
```

Figure 1: "Log Me" marking using the "logme" Session-ID header field parameter

3.2. Starting and Stopping Logging

A proxy or user agent needs to determine when it needs to mark a SIP request or response for logging. A user agent or proxy adds a "log me" marker in a request or response for two reasons: either it is configured to do so or it has detected that a dialog is being "log me" marked and maintains state to ensure that all requests and responses in the dialog are "log me" marked. During regression testing, a proxy or user agent might be configured to mark all SIP dialogs created during a given time period whereas during troubleshooting it might be configured to mark a dialog based on criteria specific to a reported fault such as calling and called party numbers. When configuration has caused a user agent or proxy to start "log me" marking requests and responses, marking continues until the dialog ends.

3.3. Identifying Test Cases

The local Universally Unique Identifier (UUID) portion of Session-ID [RFC7989] in the initial SIP request of a dialog is used as a random test case identifier. This provides the ability to collate all logged SIP requests and responses to the initial SIP request in a dialog or standalone transaction.

3.4. Passing the Marker

3.4.1. To and From a User Device

Edge proxy or B2BUA checks whether the user device is allowed to make/receive e.g. calls, based on authentication and on authorization. "Log me" marking to and from authorized devices MUST be passed unchanged.

3.4.2. To and From an External Network

An external network is a peer network connected at a network boundary as defined in [RFC8123].

External networks may be connected directly or via a peering network and such networks SHOULD have specific connection agreements. Whether "log me" marking is removed depends upon the policy applied at the network to network interface. Peer networks SHOULD endeavor to make agreements to pass "log me" marking unchanged. However, since a "log me" marker may cause a SIP entity to log the SIP header and body of a request or response, if no agreement exists between peer networks then the "log me" marker MUST be removed at a network boundary.

3.5. Logging Multiple Simultaneous Dialogs

An originating or terminating user agent and SIP entities on the signaling path can log multiple SIP dialogs simultaneously, these dialogs are differentiated by their test identifier.

3.6. Format of Logged Signaling

The entire SIP message (SIP headers and message body) is logged. Logging SHOULD use common standard formats such as the SIP CLF defined in [RFC6873] and Libpcap. If SIP CLF format is used, the entire message is logged using Vendor-ID = 00000000 and Tag = 02 in the <OptionalFields> portion of the SIP CLF record (see [RFC6873] clause 4.4). Header fields SHOULD be logged in the form in which they appear in the message, they SHOULD NOT be converted between long and compact forms described in [RFC3261] clause 7.3.3.

3.7. Marking Related Dialogs

"Log me" marking is done per-dialog and typically begins at dialog creation and ends when the dialog ends. However, dialogs related to a "log me" marked dialog MAY also be "log me" marked. An example is call transfer described in section 6.1 of [RFC5589] and explained below. The logged signalling for related dialogs can be correlated using Session-ID values as described in section 10.1 of [RFC7989].

F1 - Transferee's UA inserts "logme" parameter in the Session-ID header of the INVITE request that creates dialog1.

F3 - Transferor's UA inserts "logme" parameter in the Session-ID header of the REFER request that creates dialog2 which is related to dialog1.

F5 - Transferee's UA inserts "logme" parameter in the Session-ID header of the INVITE request that creates dialog3 which is related to dialog1.

```
                   Transferor          Transferee             Transfer
                        |                    |                  Target
                        |          INVITE F1 |                    |
                dialog1 |<-------------------|                    |
                        |          200 OK F2 |                    |
                dialog1 |------------------->|                    |
                        |            ACK     |                    |
                dialog1 |<-------------------|                    |
                        |  INVITE (hold)     |                    |
                dialog1 |------------------->|                    |
                        |  200 OK            |                    |
                dialog1 |<-------------------|                    |
                        |  ACK               |                    |
                dialog1 |------------------->|                    |
                        |  REFER F3 (Target-Dialog:1)             |
                dialog2 |------------------->|                    |
                        |  202 Accepted      |                    |
                dialog2 |<-------------------|                    |
                        | NOTIFY (100 Trying) F4                  |
                dialog2 |<-------------------|                    |
                        |            200 OK  |                    |
                dialog2 |------------------->|                    |
                        |                    |  INVITE F5         |
                dialog3 |                    |------------------->|
                        |                    |  200 OK            |
                dialog3 |                    |<-------------------|
                        |                    |  ACK               |
                dialog3 |                    |------------------->|
                        |  NOTIFY (200 OK) F6|                    |
                dialog2 |<-------------------|                    |
                        |            200 OK  |                    |
                dialog2 |------------------->|                    |
                        |  BYE               |                    |
                dialog1 |------------------->|                    |
                        |  200 OK            |                    |
                dialog1 |<-------------------|                    |
                        |                    |             BYE    |
                dialog3 |                    |<-------------------|
                        |                    |             200 OK |
                dialog3 |                    |------------------->|
```

Figure 2: "Log me" marking related dialogs in call transfer

3.8. Forked Requests

The "log me" marker MUST be copied into forked requests.

4. SIP Entity Behavior

"Log me" marking is initiated on a dialog creating side controlled by configuration. The dialog terminating side detects an incoming "log me" marker and reacts accordingly.

4.1. Endpoints

A common scenario is to have both originating and terminating endpoints support "log me" marking specification with the originating endpoint configured to initiate "log me" marking. In this simplest use case, the originating user agent inserts a "log me" marker in the dialog-creating SIP request and all subsequent SIP requests within that dialog. The "log me" marker is passed through the SIP intermediaries and arrives at the terminating user agent which ecohes "log me" header in the corresponding responses. If the terminating user agent sends an in-dialog request on a dialog that is being "log me" marked, it inserts a "log me" marker and the originating user agent echoes the "log me" marker in responses. This basic use case suggests the following principles:

- The originating user agent configured for "log me" marking logs its own signaling and inserts a "log me" marker into the dialog-creating SIP request and subsequent in-dialog SIP requests.

- The terminating user agent detects that a dialog is of interest to logging by the existence of a "log me" marker in an incoming dialog-creating SIP request.

- The terminating user agent logs marked requests and corresponding responses if allowed as per policy.

- The terminating user agent MUST echo a "log me" marker in responses to a SIP request that included a "log me" marker.

- If the terminating user agent has detected that a dialog is being "log me" marked, it MUST insert a "log me" marker in any in-dialog SIP requests that it sends.

4.2. SIP Intermediaries

A network operator may know that some of the user agents connected to the network do not support "log me" marking. In order to test sessions involving such user agents, the SIP intermediary closest to

the user agent (e.g. edge proxies, B2BUA) on the originating and terminating sides insert the "log me" marker instead. The "log me" marker is carried to the terminating user agent but it is not able to echo the "log me" marker in responses to that request. Therefore the SIP intermediary closest to the terminating user agent inserts a "log me" marker in responses to the request. Likewise, if the terminating user agent sends an in-dialog request, the SIP intermediary at the termination side inserts a "log me" marker and the SIP intermediary at the origination side echoes the "log me" marker in responses to that request. This scenario suggests the following principles when a SIP intermediary is configured to initiate or handle "log me" marking on behalf of user agent:

- The originating SIP intermediary at the originating side MUST insert a "log me" marker into SIP requests for session setup.

- The terminating SIP intermediary detects that a dialog is of interest to logging by the existence of a "log me" marker in an incoming SIP request.

- The terminating SIP intermediary logs marked requests and corresponding responses if allowed as per policy.

- The terminating SIP intermediary MUST echo a "log me" marker in responses to a SIP request that included a "log me" marker.

- If terminating SIP intermediary has detected that a dialog is being "log me" marked, it inserts a "log me" marker in in-dialog SIP requests from the terminating user agent.

- The originating SIP intermediary echoes the "log me" marker in responses to in-dialog requests received from the terminating side.

4.2.1. B2BUAs

"Log me" marking behavior of a B2BUA needs to be consistent with its purpose of troubleshooting user problems and regression testing. For example, a B2BUA that does no more than transcoding media can simply copy "log me" marking from UAS to UAC whereas a B2BUA that performs varied and complex signaling tasks such as distributing calls in a call centre needs flexible configuration so that "log me" marking can target specific B2BUA functions.

B2BUA behavior is described below for each of the B2BUA types described in [RFC7092]. The behavior described in this clause applies only to dialogs that are being "log me" marked.

For dialogs that are being "log me" marked, all B2BUAs MUST "log me" mark in-dialog SIP requests that they generate on their own, without needing explicit configuration to do so. This rule applies to both the originating and terminating sides of a B2BUA.

4.2.1.1. Proxy-B2BUA

4.2.1.1.1. Terminating behavior

A Proxy-B2BUA SHOULD copy "log me" marking in requests and responses from its terminating to the originating side without needing explicit configuration to do so.

4.2.1.2. Signaling-only and SDP-Modifying Signaling-only

4.2.1.2.1. Terminating behavior

B2BUA configured to initiate or handle "log me" marking on behalf of user agents MUST follow the principles described in Section 4.2.

B2BUA SHOULD insert "log me" marking on new dialogs initiated in the origination side if these dialogs are related to the "log me" marked dialog handled on the termination side (e.g. a new dialog is initiated on the origination side to provide IVR treatment for an end user dialog handled in the termination side).

When a B2BUA, acting as a Session Border Controller (SBC), handles "log me" marked dialog in the termination side and initiates a related dialog in the origination side towards an external network, the "log me" marking MUST be passed or removed based on connection agreements with the external network as described in Section 3.4.2.

4.2.1.2.2. Originating behavior

Whether a signaling-only B2BUA "log me" marks SIP requests that it generates on its own SHOULD be controlled by explicit configuration of the originating side, in the same way that a UAC requires configuration to control "log me" marking.

4.2.1.3. Media Relay, Media Aware, Media Termination

"Log me" marking behavior is independent of B2BUA media-plane functionality. The behavior of signaling/media plane B2BUA roles is therefore dictated only by the signaling plane role as described in Section 4.2.1.1 and Section 4.2.1.2 in this document.

4.2.2. "Log me" Marker Processing

4.2.2.1. Stateless processing

Typically, "log me" marking will be done by an originating UA and echoed by a terminating UA. Any SIP intermediary on the signalling path between these UAs MAY be stateless and simply log any SIP request or response that contains a "log me" marker, if configured to do so.

4.2.2.2. Stateful processing

It is possible that some or all user agents connected to a SIP network do not support "log me" marking, or that "log me" marking is removed from SIP messages by the originating or terminating network. These scenarios require SIP intermediaries to maintain state to enable "log me" marking:

- The originating UA does not support "log me" marking.
- The originating network removes "log me" marking from SIP requests and responses before forwarding them from its network edge to external network.
- The terminating UA does not support "log me" marking.
- The terminating network removes "log me" marking from SIP requests and responses received from its network edge to internal network.

The sections below illustrate SIP intermediary behavior in these scenarios using [RFC3665] example call flow "Session Establishment Through Two Proxies".

4.2.2.2.1. "Log Me" marking not supported by Originating UA

Alice's user agent does not support "log me" marking and hence Proxy-1 which is the SIP intermediary closest to Alice is configured to act on behalf of Alice's user agent to "log me" mark dialogs created by Alice.

In Figure 3 below, Proxy 1 in the originating network maintains state of which dialogs are being logged in order to "log me" mark all SIP requests and responses that it receives from Alice's user agent before forwarding them to Proxy 2.

```
            [ NETWORK A          ]          [ NETWORK B         ]
            Alice           Proxy 1          Proxy 2            Bob
              |                |                |                |
              |   INVITE F1    |                |                |
              |--------------->|                |                |
              |                |                |                |
              |                |                |                |
              |     407 F2     |                |                |
              |<---------------|                |                |
              |     ACK F3     |                |                |
              |--------------->|                |                |
              |   INVITE F4    |                |                |
              |--------------->|                |                |
              |                |   INVITE F5    |                |
              |                |--------------->|                |
              |                |                |                |
              |                |                |                |
              |     100  F6    |                |   INVITE F7    |
              |<---------------|     100  F8    |--------------->|
              |                |<---------------|                |
              |                |                |     180 F9     |
              |                |    180 F10     |<---------------|
              |     180 F11    |<---------------|                |
              |<---------------|                |     200 F12    |
              |                |    200 F13     |<---------------|
              |     200 F14    |<---------------|                |
              |<---------------|                |                |
              |     ACK F15    |                |                |
              |--------------->|                |                |
              |                |                |                |
              |                |    ACK F16     |                |
              |                |--------------->|                |
              |                |                |                |
              |                |                |     ACK F17    |
              |                |                |--------------->|
              |                Both Way RTP Media                |
              |<================================================>|
              |                |                |     BYE F18    |
              |                |    BYE F19     |<---------------|
              |     BYE F20    |<---------------|                |
              |<---------------|                |                |
              |     200 F21    |                |                |
              |--------------->|                |                |
              |                |     200 F22    |                |
              |                |--------------->|                |
              |                |                |                |
              |                |                |     200 F23    |
              |                |                |--------------->|
```

```
              |                |                |                |
```

Figure 3: Case 1: The originating UA does not support "log me" marking

F1 - Alice's UA does not insert a "log me" marker in the dialog-creating INVITE request F1. Nevertheless, Proxy 1 is configured to detect the start of logging. Proxy 1 logs INVITE request F1 and maintains state that this dialog is being logged.

F2 - Proxy 1 inserts a "log me" marker in INVITE request F5 before forwarding it to Proxy 2.

F3 - Proxy 1 inserts a "log me" marker in ACK request F16 before forwarding it to Proxy 2).

4.2.2.2.2. "Log Me" marking removed by Originating Network

If network A in In Figure 4 below is performing testing independently of network B then network A removes "log me" marking from SIP requests and responses forwarded to network B to prevent triggering unintended logging in network B. Proxy 1 removes "log me" marking from requests and responses that it forwards to Proxy 2 and maintains state of which dialogs are being "log me" marked in order to "log me" mark requests and responses that it forwards from Proxy 2 to Alice's user agent. Proxy 1 also logs requests and responses for the duration of the dialog.

```
              [ NETWORK A           ]          [ NETWORK B          ]
               Alice           Proxy 1          Proxy 2            Bob
                 |                |                |                |
                 |   INVITE F1    |                |                |
                 |--------------->|                |                |
                 |                |                |                |
                 |                |                |                |
                 |     407 F2     |                |                |
                 |<---------------|                |                |
                 |     ACK F3     |                |                |
                 |--------------->|                |                |
                 |   INVITE F4    |                |                |
                 |--------------->|                |                |
                 |                |INVITE F5       |                |
                 |                |--------------->|                |
                 |                |                |                |
                 |                |                |                |
                 |     100  F6    |                |                |
```

```
                    |<---------------|                |                |
                    |                |                |                |
                    |                |                |                |
                    |                |                |   INVITE F7    |
                    |                |     100  F8    |--------------->|
                    |                |<---------------|                |
                    |                |                |     180 F9     |
                    |                |    180 F10     |<---------------|
                    |                |<---------------|                |
                    |     180 F11    |                |                |
                    |<---------------|                |                |
                    |                |                |                |
                    |                |                |                |
                    |                |                |     200 F12    |
                    |                |    200 F13     |<---------------|
                    |     200 F14    |<---------------|                |
                    |<---------------|                |                |
                    |     ACK F15    |                |                |
                    |--------------->|                |                |
                    |                |    ACK F16     |                |
                    |                |--------------->|                |
                    |                |                |                |

                    |                |                |                |
                    |                |                |     ACK F17    |
                    |                |                |--------------->|
                    |                Both Way RTP Media                |
                    |<================================================>|
                    |                |                |     BYE F18    |
                    |                |    BYE F19     |<---------------|
                    |     BYE F20    |<---------------|                |
                    |<---------------|                |                |
                    |     200 F21    |                |                |
                    |--------------->|                |                |
                    |                |     200 F22    |                |
                    |                |--------------->|                |
                    |                |                |                |
                    |                |                |                |
                    |                |                |     200 F23    |
                    |                |                |--------------->|
                    |                |                |                |
```

Figure 4: Case 2: The originating network removes "log me" marking
from outgoing SIP messages at its network edge.

F1 - Alice's UA inserts a "log me" marker in the dialog-creating INVITE request and Proxy 1 therefore maintains state that this dialog is to be logged.

F5 - Proxy 1 removes "log me" marking from INVITE request before forwarding it to Proxy 2.

F6 - Proxy 1 inserts a "log me" marker in 100 response sent to the Alice's user agent.

F11 - Proxy 1 inserts a "log me" marker in 180 response before forwarding it to Alice's user agent. The same applies to responses F14, F20.

F16 - Proxy 1 removes "log me" marking from ACK request before forwarding it to Proxy 2.

F22 - Proxy 1 removes "log me" marking from the 200 response of the BYE request before forwarding it to Proxy 2.

4.2.2.2.3. "Log Me" marking not supported by Terminating UA

In Figure 5 below Bob's UA does not support "log me" marking, so Proxy 2 in the terminating network maintains state to ensure "log me" marking of SIP requests and responses from Bob's UA.

```
               [ NETWORK A           ]          [ NETWORK B          ]
               Alice           Proxy 1          Proxy 2            Bob
                 |                |                |                |
                 |   INVITE F1    |                |                |
                 |--------------->|                |                |
                 |                |                |                |
                 |                |                |                |
                 |     407 F2     |                |                |
                 |<---------------|                |                |
                 |     ACK F3     |                |                |
                 |--------------->|                |                |
                 |   INVITE F4    |                |                |
                 |--------------->|                |                |
                 |                |    INVITE F5   |                |
                 |                |--------------->|                |
                 |                |                |                |
                 |                |                |                |
                 |     100  F6    |                |                |
                 |<---------------|                |                |
                 |                |                |   INVITE F7    |
                 |                |     100  F8    |--------------->|
                 |                |<---------------|                |
```

```
                 |                |                |     180 F9     |
                 |                |                |<---------------|
                 |                |                |                |
                 |                |                |                |
                 |                |    180 F10     |                |
                 |                |<---------------|                |
                 |                |                |                |
                 |                |                |                |
                 |     180 F11    |                |                |
                 |<---------------|                |     200 F12    |
                 |                |    200 F13     |<---------------|
                 |     200 F14    |<---------------|                |
                 |<---------------|                |                |
                 |     ACK F15    |                |                |
                 |--------------->|
                 |                |    ACK F16     |                |
                 |                |--------------->|     ACK F17    |
                 |                |                |--------------->|
                 |                Both Way RTP Media                |
                 |<=================================================>|
                 |                |                |     BYE F18    |
                 |                |    BYE F19     |<---------------|
                 |     BYE F20    |<---------------|                |
                 |<---------------|                |                |
                 |     200 F21    |                |                |
                 |--------------->|
                 |                |     200 F22    |                |
                 |                |--------------->|     200 F23    |
                 |                |                |--------------->|
                 |                |                |                |
```

Figure 5: Case 3: The terminating UA does not support "log me" marking.

F1 - Alice's UA inserts a "log me" marker in the the dialog-creating INVITE request F1.

F5 - INVITE F5 is "log me" marked and Proxy 2 therefore maintains state that this dialog is to be logged.

F9 - Bob's UA does not support "log me" marking, therefore the 180 response to the INVITE request doesn't have a "log me" marker.

F10 - Proxy 2 inserts a "log me" marker in the 180 response on behalf of Bob's UA before forwarding it. The same applies to response F13 and BYE request in F19.

4.2.2.2.4. "Log Me" marking removed by Terminating Network

In Figure 6 below Proxy 2 removes "log me" marking from all SIP requests and responses entering network B. Proxy 1 therefore maintains state of which dialogs are being "log me" marked in order to "log me" mark all requests and responses that it receives from Proxy 2.

```
               [ NETWORK A           ]          [ NETWORK B          ]
               Alice           Proxy 1          Proxy 2            Bob
                 |                |                |                |
                 |   INVITE F1    |                |                |
                 |--------------->|                |                |
                 |                |                |                |
                 |     407 F2     |                |                |
                 |<---------------|                |                |
                 |     ACK F3     |                |                |
                 |--------------->|                |                |
                 |   INVITE F4    |                |                |
                 |--------------->|                |                |
                 |                |    INVITE F5   |                |
                 |                |--------------->|                |
                 |                |                |                |
                 |                |                |                |
                 |     100  F6    |                |                |
                 |<---------------|                |                |
                 |                |                |   INVITE F7    |
                 |                |     100  F8    |--------------->|
                 |                |<---------------|                |
                 |                |                |     180 F9     |
                 |                |                |<---------------|
                 |                |    180 F10     |
                 |                |<---------------|                |
                 |                |                |                |

                 |                |                |                |
                 |     180 F11    |                |                |
                 |<---------------|                |     200 F12    |
                 |                |    200 F13     |<---------------|
                 |     200 F14    |<---------------|                |
                 |<---------------|                |                |
                 |     ACK F15    |                |                |
                 |--------------->|
```

```
                 |                |    ACK F16     |                |
                 |                |--------------->|     ACK F17    |
                 |                |                |--------------->|
                 |                Both Way RTP Media                |
                 |<================================================>|
                 |                |                |     BYE F18    |
                 |                |    BYE F19     |<---------------|
                 |     BYE F20    |<---------------|                |
                 |<---------------|                |                |
                 |     200 F21    |                |                |
                 |--------------->|
                 |                |     200 F22    |                |
                 |                |--------------->|     200 F23    |
                 |                |                |--------------->|
                 |                |                |                |
```

Figure 6: Case 2: The terminating network removes "log me" marking from incoming SIP messages at its network edge.

F1 - Alice's UA inserts a "log me" marker in the dialog-creating INVITE request F1. Proxy 1 detects the "log me" marker and maintains state that this dialog is to be logged.

F5 - Proxy 2 removes "log me" marker in the INVITE request F5 before forwarding it as F7.

F10 - Proxy 1 inserts a "log me" marker in 180 response of the INVITE request before forwarding it as F11. The same applies to responses F13 and BYE request in F19.

5. Error Handling

5.1. Missing "Log me" Marker in Dialog Being Logged

A terminating user agent or terminating edge proxy that has been echoing markers in responses for a given dialog might receive a SIP request that has not been "log me" marked. Since "log me" marking is done per dialog, this is an error. In such cases, the user agent or proxy SHOULD consider "log me" marking to have ended and MUST NOT mark a response to the unmarked request, responses to subsequent requests in the dialog, or in-dialog requests sent from the terminating side.

5.2. "Log Me" Marker Appears Mid-Dialog

"log me" marking that begins mid-dialog is an error case and the terminating user agent or edge proxy MUST NOT "log me" mark responses to the marked request, responses to subsequent requests in the dialog, or in-dialog requests from the terminating side.

6. Security Considerations

6.1. "Log Me" Authorization

An end user or network administrator MUST give permission for a terminal to perform "log me" marking. The configuration of a SIP intermediary to perform "log me" marking on behalf of a terminal MUST be authorized by the network administrator.

Activating a debug mode affects the operation of a terminal, therefore debugging configuration MUST be supplied by an authorized party to an authorized terminal through a secure communication channel.

6.2. "Log Me" Marker Removal

The log me marker is not sensitive information, although it will sometimes be inserted because a particular device is experiencing problems.

The presence of a log me marker will cause some SIP entities to log signaling messages. Therefore, this marker MUST be removed at the earliest opportunity if it has been incorrectly inserted, such as appearing mid-dialog in a dialog that was not being logged or outside the configured start and stop of logging.

If SIP requests and responses are exchanged with an external network with which there is no agreement to pass "log me" marking, then the "log me" marking is removed.

6.3. Denial of Service Attacks

Maliciously configuring a large number of terminals to simultaneously "log me" mark dialogs will cause high processor load on SIP entities that are logging signalling. Since "log me" marking is for the small number of dialogs subject to troubleshooting or regression testing, the number of dialogs that can be simultaneously logged can be statically limited without adversely affecting the usefulness of "log me" marking. Also, the SIP intermediary closest to the terminal and SIP intermediary at network edge (e.g Session Border Controllers) can

be configured to screen-out "log me" markers when troubleshooting or regression testing is not in progress.

6.4. Privacy

Logging includes all SIP header fields, the SIP privacy mechanisms defined in [RFC3323] can be used to ensure that logs do not divulge personal identity information.

6.4.1. Personal Identifiers

"Log me" marking is defined for the SIP Protocol, and SIP has header fields such as From, Contact, P-Asserted-Identity that can carry personal identifiers. Different protocol interactions can be correlated using the Session-ID and Call-ID header fields, but such correlation is limited to a single end-to-end session.

In order to protect user privacy during logging, privacy settings can be enabled or requested by the terminal used by the end user. [RFC3323] suggests two mechanisms:

- By using the value anonymous in the From header field

- By requesting privacy from SIP intermediaries using the Privacy header

"Log me" marking is typically used for troubleshooting and regression testing, and in some cases a service provider owned device with a dummy account can be used instead of a customer device. In such cases, no personal identifiers are included in the logged signaling messages.

6.4.2. Data Stored at SIP Intermediaries

SIP endpoints and intermediaries that honor the "log me" request store all the SIP messages that are exchanged within a given dialog. SIP messages can contain the personal identifiers listed in Section 6.4.1 and additionally a user identity, calling party number, IP address, hostname, and other user and device related items. The SIP message bodies describe the kind of session being set up by the identified end user and device.

"Log me" marking does not introduce any additional user or device data to SIP but might indicate that a specific user is experiencing a problem.

6.4.3. Data Visible at Network Elements

SIP messages that are logged due to "log me" requests are stored only by the SIP initiators, intermediaries and recipients. Enablers as defined in section 3.1 of [RFC6973], such as firewalls and DNS servers do not log messages due to the "log me" marking.

6.4.4. Preventing Fingerprinting

"Log me" functionality is typically used to troubleshoot a given problem and hence it can be used as an method to identify users and devices that are experiencing issues. The best way to prevent fingerprinting is to enable or request SIP privacy for the logged dialog.

6.4.5. Retaining Logs

The lifetime of "log me" marking is equivalent to the lifetime of the dialog that initiated the "log me" request. When "log me" is extended to related dialogs the lifetime is extended until there is no more related dialog for the end-to-end session.

"log me" automatically expires at the end of the dialog and there is no explicit mechanism to turn off logging within a dialog.

The scope of "log me" Marking is limited i.e. an user or the network administrator has to enable it on a per session basis or for a specific time period. This minimizes the risk of exposing user data for an indefinite time.

The retention time period for logged messages is out of scope for this document and is expected to be configured based on the data storage policies of service providers and enterprises.

6.4.6. User Control of Logging

Consent to turn on "log me" for a given session MUST be provided by the end user or by the network administrator. It is handled outside of the protocol through user interface or application programming interfaces at the end point, call control elements and network management systems.

SIP entities across the communication path can be configured to pass through the "log me" marking but not honor the request i.e. not log the data based on local policies.

6.4.7. Recommended Defaults

The recommended defaults for "log me" marking are:

- o turn on SIP privacy as described in Section 6.4 or use a service provider owned device with a dummy user identity for test calls

- o use the local UUID of Session-ID header at the originating device as the test identifier as described in Section 3.3

6.5. Data Protection

A SIP entity that has logged information MUST protect the logs. Storage of the log files are subject to the security considerations specified in [RFC6872].

7. Augmented BNF for the "logme" Parameter

ABNF is described in [RFC5234]. This document introduces a new "logme"parameter for the Session-ID header field defined in Section 5 of [RFC7989].

```
     sess-id-param       = remote-param / logme-param / generic-param

     remote-param        = "remote" EQUAL remote-uuid

     logme-param         = "logme"
```

Figure 7: Augmented BNF for the "logme" Parameter

8. IANA Considerations

8.1. Registration of the "logme" Parameter

The following parameter is to be added to the "Header Field Parameters and Parameter Values" section of the SIP parameter registry:

Header Field	Parameter Name	Predefined Values	Reference
Session-ID	logme	No	[RFCXXXX]

Table 1

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC6872] Gurbani, V., Ed., Burger, E., Ed., Anjali, T., Abdelnur, H., and O. Festor, "The Common Log Format (CLF) for the Session Initiation Protocol (SIP): Framework and Information Model", RFC 6872, DOI 10.17487/RFC6872, February 2013, <http://www.rfc-editor.org/info/rfc6872>.

[RFC6873] Salgueiro, G., Gurbani, V., and A. Roach, "Format for the Session Initiation Protocol (SIP) Common Log Format (CLF)", RFC 6873, DOI 10.17487/RFC6873, February 2013, <http://www.rfc-editor.org/info/rfc6873>.

[RFC7206] Jones, P., Salgueiro, G., Polk, J., Liess, L., and H. Kaplan, "Requirements for an End-to-End Session Identification in IP-Based Multimedia Communication Networks", RFC 7206, DOI 10.17487/RFC7206, May 2014, <http://www.rfc-editor.org/info/rfc7206>.

[RFC7989] Jones, P., Salgueiro, G., Pearce, C., and P. Giralt, "End-to-End Session Identification in IP-Based Multimedia Communication Networks", RFC 7989, DOI 10.17487/RFC7989, October 2016, <http://www.rfc-editor.org/info/rfc7989>.

9.2. Informative References

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, DOI 10.17487/RFC3323, November 2002, <http://www.rfc-editor.org/info/rfc3323>.

[RFC3665] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and K. Summers, "Session Initiation Protocol (SIP) Basic Call Flow Examples", BCP 75, RFC 3665, DOI 10.17487/RFC3665, December 2003, <http://www.rfc-editor.org/info/rfc3665>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC5589] Sparks, R., Johnston, A., Ed., and D. Petrie, "Session Initiation Protocol (SIP) Call Control - Transfer", BCP 149, RFC 5589, DOI 10.17487/RFC5589, June 2009, <http://www.rfc-editor.org/info/rfc5589>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

[RFC7092] Kaplan, H. and V. Pascual, "A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents", RFC 7092, DOI 10.17487/RFC7092, December 2013, <http://www.rfc-editor.org/info/rfc7092>.

[RFC8123] Dawes, P. and C. Arunachalam, "Requirements for Marking SIP Messages to be Logged", RFC 8123, DOI 10.17487/RFC8123, March 2017, <http://www.rfc-editor.org/info/rfc8123>.

Authors' Addresses

Peter Dawes
Vodafone Group
The Connection
Newbury, Berkshire RG14 2FN
UK

Email: peter.dawes@vodafone.com

Chidambaram Arunachalam
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC, NC 27709
US

Email: carunach@cisco.com