Network Working Group
Request for Comments: 4458
Category: Informational

C. Jennings
Cisco Systems
F. Audet
Nortel Networks
J. Elwell
Siemens plc
April 2006

Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

The Session Initiation Protocol (SIP) is often used to initiate connections to applications such as voicemail or interactive voice recognition systems. This specification describes a convention for forming SIP service URIs that request particular services based on redirecting targets from such applications.

Table of Contents

1. Introduction

Many applications such as Unified Messaging (UM) systems and Interactive Voice Recognition (IVR) systems have been developed out of traditional telephony. They can be used for storing and interacting with voice, video, faxes, email, and instant messaging services. Users often use SIP to initiate communications with these applications. When a SIP call is routed to an application, it is necessary that the application be able to obtain several bits of information from the session initiation message so that it can deliver the desired services.

For the purpose of this document, we will use UM as the main example, but other applications may use the mechanism defined in this document. The UM needs to know what mailbox should be used and possible reasons for the type of service desired from the UM. Many voicemail systems provide different greetings depending whether the call went to voicemail because the user was busy or because the user did not answer. All of this information can be delivered in existing SIP signaling from the call control that retargets the call to the UM, but there are no conventions for describing how the desired mailbox and the service requested are expressed. It would be possible for every vendor to make this configurable so that any site could get it to work; however, this approach is unrealistic for achieving interoperability among call control, gateway, and unified messaging systems from different vendors. This specification describes a convention for describing this mailbox and service information in the SIP URI so that vendors and operators can build interoperable systems.

If there were no need to interoperate with Time Division Multiplexing (TDM)-based voicemail systems or to allow TDM systems to use VoIP unified messaging systems, this problem would be a little easier to solve. The problem that is introduced in the Voice over IP (VoIP) to TDM case is as follows. The SIP system needs to tell a Public Switched Telephone Network (PSTN) gateway both the subscriber’s mailbox identifier (which typically looks like a phone number) and the address of the voicemail system in the TDM network (again a phone number).

The question has been asked why the To header cannot be used to specify which mailbox to use. One problem is that the call control proxies cannot modify the To header, and the User Agent Clients (UACs) often set it incorrectly because they do not have information about the subscribers in the domain they are trying to call. This happens because the routing of the call often translates the URI multiple times before it results in an identifier for the desired user that is valid in the namespace that the UM system understands.

2. Mechanism (User Agent Server and Proxy)

The mechanism works by encoding the information for the desired service in the SIP Request-URI that is sent to the UM system. Two chunks of information are encoded, the first being the target mailbox to use and the second being the SIP status code that caused this retargeting and that indicates the desired service. The userinfo and hostport parts of the Request-URI will identify the voicemail service, the target mailbox can be put in the target parameter, and the reason can be put in the cause parameter. For example, if the proxy wished to use Bob's mailbox because his phone was busy, the URI sent to the UM system could be something like:

sip:voicemail@example.com;target=bob%40example.com;cause=486

2.1. Target

Target is a URI parameter that indicates the address of the retargeting entity: in the context of UM, this can be the mailbox number. For example, in the case of a voicemail system on the PSTN, the user portion will contain the phone number of the voicemail system, while the target will contain the phone number of the subscriber's mailbox.

2.2. Cause

Cause is a URI parameter that is used to indicate the service that the User Agent Server (UAS) receiving the message should perform. The following values for this URI parameter are defined:

Redirecting Reason	Value
Unknown/Not available	404
User busy	486
No reply	408
Unconditional	302
Deflection during alerting	487
Deflection immediate response	480
Mobile subscriber not reachable	503

The mapping to PSTN protocols is important both for gateways that connect the IP network to existing TDM customer's equipment, such as Private Branch Exchanges (PBXs) and voicemail systems, and for gateways that connect the IP network to the PSTN network. Integrated Services Digital Network User Part (ISUP) has signaling encodings for

this information that can be treated as roughly equivalent for the purposes here. For this reason, this specification uses the names of Redirecting Reason values defined in ITU-T Q.732.2-5 [8]. In this specification, the Redirecting Reason Values are referred to as "Causes". It should be understood that the term "Cause" has nothing to do with PSTN "Cause values" (as per ITU-T Q.850 [9] and RFC 3398 [5]) but are instead mapped to ITU-T Q.732.2-5 Redirecting Reasons. Since ISUP interoperates with other PSTN networks, such as Q.931 [10] and QSIG [11], using well-known rules, it makes sense to use the ISUP names as the most appropriate superset. If no appropriate mapping to a cause value defined in this specification exists in a network, it would be mapped to 302 "Unconditional". Similarly, if the mapping occurs from one of the causes defined in this specification to a PSTN system that does not have an equivalent reason value, it would be mapped to that network's equivalent of "Unconditional". If a new cause parameter needs to be defined, this specification will have to be updated.

The user portion of the URI SHOULD be used as the address of the voicemail system on the PSTN, while the target SHOULD be mapped to the original redirecting number on the PSTN side.

The redirection counters SHOULD be set to one unless additional information is available.

2.3. Retrieving Messages

The UM system MAY use the fact that the From header is the same as the URI target as a hint that the user wishes to retrieve messages.

3. Interaction with Request History Information

The Request History mechanism [6] provides more information relating to multiple retargetings. It is reasonable to have systems in which both the information in this specification and the History information are included and one or both are used.

History-Info specifies a means of providing the UAS and UAC with information about the retargeting of a request. This information includes the initial Request-URI and any retarget-to URIs. This information is placed in the History-Info header field, which, except where prevented by privacy considerations, is built up as the request progresses and, upon reaching the UAS, is returned in certain responses.

History-Info, when deployed at relevant SIP entities, is intended to provide a comprehensive trace of retargeting for a SIP request, along with the SIP response codes that led to retargeting.

History-Info can complement this specification. In particular, when a proxy inserts a URI containing the parameters defined in this specification into the Request-URI of a forwarded request, the proxy can also insert a History-Info header field entry into the forwarded request, and the URI in that entry will incorporate these parameters. Therefore, even if the Request-URI is replaced as a result of rerouting by a downstream proxy, the History-Info header field will still contain these parameters, which may be of use to the UAS. Consequently, UASes that make use of this information may find the information in the History-Info header and/or in the Request-URI, depending on the capability of the proxy to support generation of History-Info or on the behavior of downstream proxies; therefore, applications need to take this into account.

4. Limitations of Voicemail URI

This specification requires the proxy that is requesting the service to understand whether the UM system it is targeting supports the syntax defined in this specification. Today, this information is provided to the proxy by configuration. For practical purposes, this means that the approach is unlikely to work in cases in which the proxy is not configured with information about the UM system or in which the UM is not in the same administrative domain.

This approach only works when the service that the call control wants applied is fairly simple. For example, it does not allow the proxy to express information like "Do not offer to connect to the target's colleague because that address has already been tried".

The limitations discussed in this section are addressed by History-Info [6].

5. Syntax

The ABNF[4] grammar for these parameters is shown below. The definitions of pvalue and Status-Code are defined in the ABNF in RFC 3261[1].

```
target-param      =  "target" EQUAL pvalue

cause-param       =  "cause" EQUAL Status-Code
```

Note that the ABNF requires some characters to be escaped if they occur in the value of the target parameters. For example, the "@" character needs to be escaped.

6. Examples

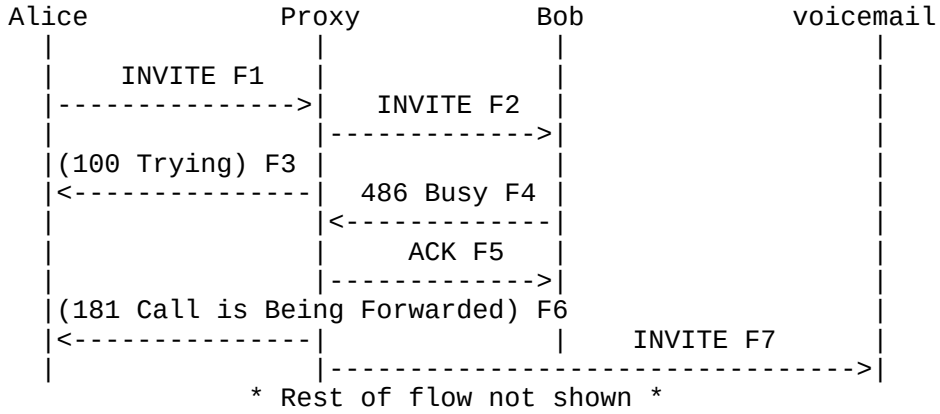
This section provides some example use cases for the solution proposed in this document. For the purpose of this document, UM is used as the main example, but other applications may use this mechanism. The examples are intended to highlight the potential applicability of this solution and are not intended to limit its applicability.

Also, the examples show just service retargeting on busy, but can easily be adapted to show other forms of retargeting.

In several of the examples, the URIs are broken across more than one line. This was only done for formatting and is not a valid SIP message. Some of the characters in the URIs are not correctly escaped to improve readability. The examples are all shown using sip: with UDP transport, for readability. It should be understood that using sips: with TLS transport is preferable.

6.1. Proxy Forwards Busy to Voicemail

In this example, Alice calls Bob. Bob's proxy determines that Bob is busy, and the proxy forwards the call to Bob's voicemail. Alice's phone is at 192.0.2.1, while Bob's phone is at 192.0.2.2. The important thing to note is the URI in message F7.



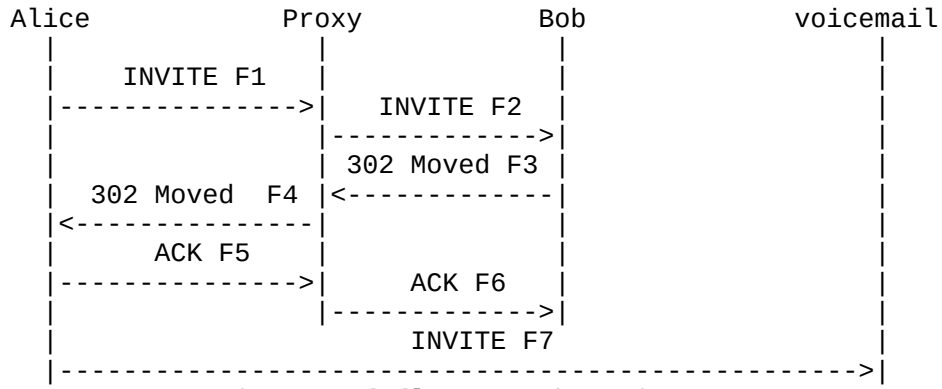
```
    F1: INVITE 192.0.2.1 -> proxy.example.com

    INVITE sip:+15555551002@example.com;user=phone  SIP/2.0
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Max-Forwards: 70
    Contact: <sip:alice@192.0.2.1>
    Content-Type: application/sdp
    Content-Length: *Body length goes here*

    * SDP goes here*


    F2: INVITE proxy.example.com -> 192.0.2.2

    INVITE sip:+15555551002@192.0.2.2 SIP/2.0
    Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-1
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Max-Forwards: 70
    Contact: <sip:alice@192.0.2.1>
    Content-Type: application/sdp
    Content-Length: *Body length goes here*

    * SDP goes here*


    F4: 486 192.0.2.2 -> proxy.example.com

    SIP/2.0 486 Busy Here
    Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-1
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone;tag=09xde23d80
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Content-Length: 0
```

F7: INVITE proxy.example.com -> um.example.com

```
INVITE sip:voicemail@example.com;\
       target=sip:+15555551002%40example.com;user=phone;\
       cause=486  SIP/2.0
Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.0.2.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

6.2. Endpoint Forwards Busy to Voicemail

In this example, Alice calls Bob. Bob is busy, but forwards the session directly to his voicemail. Alice's phone is at 192.0.2.1, while Bob's phone is at 192.0.2.2. The important thing to note is the URI in the Contact in message F3.



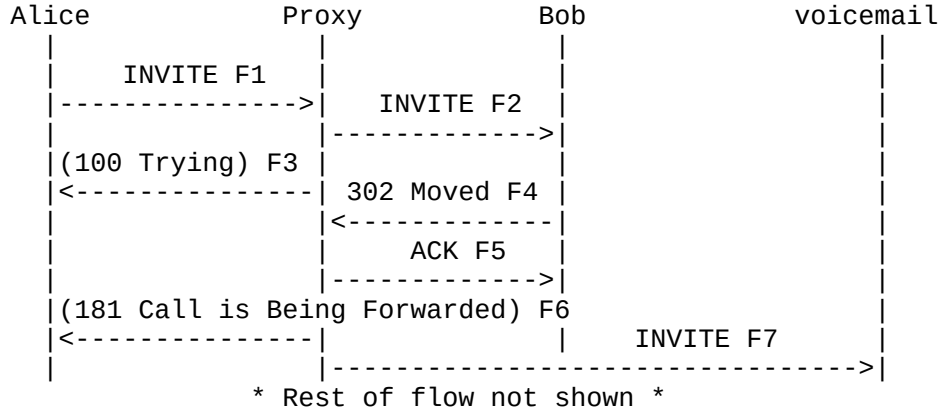
```
    F1: INVITE 192.0.2.1 -> proxy.example.com

    INVITE sip:+15555551002@example.com;user=phone  SIP/2.0
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Max-Forwards: 70
    Contact: <sip:alice@192.0.2.1>
    Content-Type: application/sdp
    Content-Length: *Body length goes here*

    * SDP goes here*


    F2: INVITE proxy.example.com -> 192.0.2.2

    INVITE sip:line1@192.0.2.2 SIP/2.0
    Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-1
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Max-Forwards: 70
    Contact: <sip:alice@192.0.2.1>
    Content-Type: application/sdp
    Content-Length: *Body length goes here*

    * SDP goes here*


    F3: 302 192.0.2.2 -> proxy.example.com

    SIP/2.0 302 Moved Temporarily
    Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-1
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone;tag=09xde23d80
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Contact: <sip: voicemail@example.com;\
           target=sip:+15555551002%40example.com;user=phone;\
           cause=486;>
    Content-Length: 0
```

```
F7: INVITE proxy.example.com -> um.example.com

INVITE sip: voicemail@example.com;\
       target=sip:+15555551002%40example.com;user=phone;\
       cause=486  SIP/2.0
Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.0.2.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

6.3. Endpoint Forwards Busy to TDM via a Gateway

In this example, the voicemail is reached via a gateway to a TDM network. Bob's number is +1 555 555-1002, while voicemail's number on the TDM network is +1-555-555-2000.

The call flow is the same as in Section 6.2 except for the Contact URI in F4 and the Request URI in F7.



```
    F4: 486 192.0.2.2 -> proxy.example.com

    SIP/2.0 302 Moved temporarily
    Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-1
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone;tag=09xde23d80
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Contact: <sip:+15555552000@example.com;user=phone;\
              target=tel:+15555551002;cause=486>
    Content-Length: 0


    F7: INVITE proxy.example.com -> gw.example.com

    INVITE sip:+15555552000@example.com;user=phone;\
           target=tel:+15555551002;cause=486\
           SIP/2.0
    Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-2
    Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
    From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
    To: sip:+15555551002@example.com;user=phone
    Call-ID: c3x842276298220188511
    CSeq: 1 INVITE
    Max-Forwards: 70
    Contact: <sip:alice@192.0.2.1;transport=tcp>
    Content-Type: application/sdp
    Content-Length: *Body length goes here*

    * SDP goes here*
```

6.4. Endpoint Forwards Busy to Voicemail with History Info

This example illustrates how History Info works in conjunction with service retargeting. The scenario is the same as Section 6.1.

```
F1: INVITE 192.0.2.1 -> proxy.example.com

INVITE sip:+15555551002@example.com;user=phone  SIP/2.0
Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.0.2.1>
History-Info: <sip:+15555551002@example.com;user=phone >;index=1
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*


F2: INVITE proxy.example.com -> 192.0.2.2

INVITE sip:line1@192.0.2.2 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-1
Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.0.2.1>
History-Info: <sip:+15555551002@example.com;user=phone >;index=1,
              <sip:line1@192.0.2.4>;index=1.1

Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

```
F7: INVITE proxy.example.com -> um.example.com

INVITE sip: voicemail@example.com;\
       target=sip:+15555551002%40example.com;user=phone;\
       cause=486  SIP/2.0
Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.0.2.1>
History-Info: <sip:+15555551002@example.com;user=phone >;index=1,
              <sip:line1@192.0.2.4?Reason=SIP%3Bcause%3D302;\
               text="Moved Temporarily">;index=1.1
              <sip: voicemail@example.com;\
               target=sip:+15555551002%40example.com;user=phone;\
               cause=486>;index=2
Contact: <sip:alice@192.0.2.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

6.5. Zero Configuration UM System

In this example, the UM system has no configuration information specific to any user. The proxy is configured to pass a URI that provides the prompt to play and an email address in the user portion of the URI to which the recorded message is to be sent.

The call flow is the same as in Section 6.1, except that the URI in F7 changes to specify the user part as Bob’s email address, and the Netann [7] URI play parameter specifies where the greeting to play can be fetched from.

```
F7: INVITE proxy.example.com -> voicemail.example.com

INVITE sip:voicemail@example.com;target=mailto:bob%40example.com;\
   cause=486;play=http://www.example.com/bob/busy.wav SIP/2.0
Via: SIP/2.0/TCP 192.0.2.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.0.2.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15555551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.0.2.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

In addition, if the proxy wished to indicate a Voice XML (VXML) script that the UM should execute, it could add a parameter to the URI in the above message that looked like:

```
voicexml=http://www.example.com/bob/busy.vxml
```

6.6. Call Coverage

In a Call Coverage example, a user on the PSTN calls an 800 number. The gateway sends this to the proxy, which recognizes that the helpdesk is the target. Alice and Bob are staffing the help desk and are tried sequentially, but neither answers, so the call is forwarded to the helpdesk's voicemail.

The details of this flow are trivial and not shown. The key item in this example is that the INVITE to Alice and Bob looks as follows:

```
INVITE sip:voicemail@example.com;target=helpdesk%40example.com;\
       cause=302 SIP/2.0
```

7. IANA Considerations

This specification adds two new values to the IANA registration in the "SIP/SIPS URI Parameters" registry as defined in [3].

Parameter Name	Predefined Values	Reference
target	No	[RFC4458]
cause	Yes	[RFC4458]

8. Security Considerations

This document discusses transactions involving at least three parties, which increases the complexity of the privacy issues.

The new URI parameters defined in this document are generally sent from a Proxy or call control system to a Unified Messaging (UM) system or to a gateway to the PSTN and then to a voicemail system. These new parameters tell the UM what service the proxy wishes to have performed. Just as any message sent from the proxy to the UM needs to be integrity protected, these messages need to be integrity protected to stop attackers from, for example, causing a voicemail meant for a company's CEO to go to an attacker's mailbox. RFC 3261 provides a TLS mechanism suitable for performing this integrity protection.

The signaling from the Proxy to the UM or gateway will reveal who is calling whom and possibly some information about a user's presence based on whether the call was answered or sent to voicemail. This information can be protected by encrypting the SIP traffic between the Proxy and UM or gateway. Again, RFC 3261 contains mechanisms for accomplishing this using TLS.

Implementations should implement and use TLS.

8.1. Integrity Protection of Forwarding in SIP

The forwarding of a call in SIP brings up a very strange trust issue. Consider the normal case -- A calls B and the call gets forwarded to C by a network element in B's domain, and then C answers the call. A has called B but ended up talking to C. This scenario may be hard to separate from a man-in-the-middle attack.

There are two possible solutions. One is that B sends back information to A saying don't call me, call C, and signs it as B. The problem is that this solution involves revealing that B has forwarded to C, which B often may not want to do. For example, B may be a work phone that has been forwarded to a mobile or home phone. The user does not want to reveal their mobile or home phone number but, even more importantly, does not want to reveal that they are not in the office.

The other possible solution is that A needs to trust B only to forward to a trusted identity. This requires a hop-by-hop transitive trust such that each hop will only send to a trusted next hop and each hop will only do things that the user at that hop desired. This

solution is enforced in SIP using the SIPS URI and TLS-based hop-by-hop security. It protects from an off-axis attack, but if one of the hops is not trustworthy, the call may be diverted to an attacker.

Any redirection of a call to an attacker's mailbox is serious. It is trivial for an attacker to make its mailbox seem very much like the real mailbox and forward the messages to the real mailbox so that the fact that the messages have been intercepted or even tampered with escapes detection. Approaches such as the SIPS URL and the History-Info[6] can help protect against these attacks.

8.2. Privacy Related Issues on the Second Call Leg

In the case where A calls B and gets redirected to C, occasionally people suggest that there is a requirement for the call leg from B to C to be anonymous. The SIP case is not the PSTN, and there is no call leg from B to C; instead, there is a VoIP session between A and C. If A has put a To header field value containing B in the initial invite message, unless something special is done about it, C would see that To header field value. If the person who answers phone C says "I think you dialed the wrong number; who were you trying to reach?", A will probably specify B.

If A does not want C to see that the call was to B, A needs a special relationship with the forwarding Proxy to induce it not to reveal that information. The call should go through an anonymization service that provides session or user level privacy (as described in RFC 3323 [2]) service before going to C. It is not hard to figure out how to meet this requirement, but it is unclear why anyone would want this service.

The scenario in which B wants to make sure that C does not see that the call was to B is easier to deal with but a bit weird. The usual argument is that Bill wants to forward his phone to Monica but does not want Monica to find out his phone number. It is hard to imagine that Monica would want to accept all Bill's calls without knowing how to call Bill to complain. The only person Monica will be able to complain to is Hillary, when she tries to call Bill. Several popular web portals will send SMS alert messages about things like stock prices and weather to mobile phone users today. Some of these contain no information about the account on the web portal that initiated them, making it nearly impossible for the mobile phone owner to stop them. This anonymous message forwarding has turned out to be a really bad idea even where no malice is present. Clearly some people are fairly dubious about the need for this, but never mind: let's look at how it is solved.

In the general case, the proxy needs to route the call through an anonymization service and everything will be cleaned up. Any anonymization service that performs the "Privacy: Header" Service in RFC 3323 [2] must remove the cause and target URI parameters from the URI. Privacy of the parameters, when they form part of a URI within the History-Info header, is covered in History-Info [6].

This specification does not discuss the security considerations of mapping to a PSTN Gateway. Security implications of mapping to ISUP, for example, are discussed in RFC 3398 [5].

9. Acknowledgements

Many thanks to Mary Barnes, Steve Levy, Dean Willis, Allison Mankin, Martin Dolly, Paul Kyzivat, Erick Sasaki, Lyndsay Campbell, Keith Drage, Miguel Garcia, Sebastien Garcin, Roland Jesske, Takumi Ohba, and Rohan Mahy.

10. References

10.1. Normative 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] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[3] Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)", BCP 99, RFC 3969, December 2004.

[4] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

10.2. Informative References

[5] Camarillo, G., Roach, A., Peterson, J., and L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping", RFC 3398, December 2002.

[6] Barnes, M., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

[7] Burger, E., Van Dyke, J., and A. Spitzer, "Basic Network Media Services with SIP", RFC 4240, December 2005.

[8] "Stage 3 description for call offering supplementary services using signalling system No. 7: Call diversion services", ITU-T Recommendation Q.732.2-5, December 1999.

[9] "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part", ITU-T Recommendation Q.850, May 1998.

[10] "ISDN user-network interface layer 3 specification for basic call control", ITU-T Recommendation Q.931, May 1998.

[11] "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit mode bearer services - Inter-exchange signalling procedures and protocol", ISO/IEC 11572, March 2000.

Authors' Addresses

Cullen Jennings
Cisco Systems
170 West Tasman Drive
Mailstop SJC-21/2
San Jose, CA 95134
USA

Phone: +1 408 421-9990
EMail: fluffy@cisco.com

Francois Audet
Nortel Networks
4655 Great America Parkway
Santa Clara, CA 95054
US

Phone: +1 408 495 3756
EMail: audet@nortel.com

John Elwell
Siemens plc
Technology Drive
Beeston, Nottingham NG9 1LA
UK

EMail: john.elwell@siemens.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).