Internet Engineering Task Force (IETF)
Request for Comments: 8197
Category: Standards Track
ISSN: 2070-1721

H. Schulzrinne
FCC

July 2017

A SIP Response Code for Unwanted Calls

Abstract

This document defines the 607 (Unwanted) SIP response code, allowing called parties to indicate that the call or message was unwanted. SIP entities may use this information to adjust how future calls from this calling party are handled for the called party or more broadly.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8197.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

In many countries, an increasing number of calls are unwanted [RFC5039]: they might be fraudulent or illegal telemarketing or maybe the receiving party does not want to be disturbed by, say, surveys or solicitation by charities. Carriers and other service providers may want to help their subscribers avoid receiving such calls, using a variety of global or user-specific filtering algorithms. One input into such algorithms is user feedback. User feedback may be offered through smartphone apps, APIs or within the context of a SIP-initiated call. This document addresses feedback within the SIP call. Here, the called party either rejects the SIP [RFC3261] request as unwanted or terminates the session with a BYE request after answering the call. INVITE and MESSAGE requests are most likely to trigger such a response.

To allow the called party to express that the call was unwanted, this document defines the 607 (Unwanted) response code. The user agent (UA) of the called party, based on input from the called party or some UA-internal logic, uses this to indicate that this call is unwanted and that future attempts are likely to be similarly rejected. While factors such as identity spoofing and call forwarding may make authoritative identification of the calling party difficult or impossible, the network can use such a rejection -- possibly combined with a pattern of rejections by other callees and/or other information -- as input to a heuristic algorithm for determining future call treatment. The heuristic processing and possible treatment of persistently unwanted calls are outside the scope of this document.

When this document refers to "caller identity", it uses "identity" in the same sense as [SIP-IDENTITY], i.e., to mean either a canonical address-of-record (AOR) SIP URI employed to reach a user (such as 'sip:alice@atlanta.example.com'), or a telephone number, which commonly appears in either a tel URI [RFC3966] or as the user portion of a SIP URI.

2. Normative Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Motivation

None of the existing 4xx, 5xx, or 6xx response codes signify that this SIP request is unwanted by the called party. For example, 603 (Decline) might be used if the called party is currently at dinner or in a meeting, but does not want to indicate any specific reason. As described in Section 21.6.2 [RFC3261], a 603 response may include a Retry-After header field to indicate a better time to attempt the call. Thus, the call is rejected due to the called party's (temporary) status. As described in Section 4, the called party invokes the "unwanted call" user interface and 607 (Unwanted) response indicating that it is instead the caller's identity that is causing the call to be rejected.

4. Behavior of SIP Entities

The response code 607 MAY be used in a failure response for an INVITE, MESSAGE, SUBSCRIBE, or other out-of-dialog SIP request to indicate that the offered communication is unwanted. The response code MAY also be used as the value of the "cause" parameter of a SIP reason-value in a Reason header field [RFC3326], typically when the called party user agent issues a BYE request terminating an incoming call or a forking proxy issues a CANCEL request after receiving a 607 response from one of the branches. (Including a Reason header field with the 607 status code allows the called party user agent that receives a CANCEL request to make an informed choice whether and how to include such calls in their missed-call list or whether to show an appropriate indication to the user.)

The SIP entities receiving this response code are not obligated to take any particular action beyond those appropriate for 6xx responses. Following the default handling for 6xx responses in [RFC5057], the 607 response destroys the transaction. The service provider delivering calls or messages to the user issuing the response MAY take a range of actions, for example, add the calling party to a personal blacklist specific to the called party, use the information as input when computing the likelihood that the calling party is placing unwanted calls ("crowd sourcing"), initiate a traceback request, or report the calling party's identity to consumer complaint databases. As discussed in Section 6, reversing the 'unwanted' labeling is beyond the scope of this mechanism, as it will likely require a mechanism other than call signaling.

The user experience is envisioned to be somewhat similar to email spam buttons where the detailed actions of the email provider remain opaque to the user.

The mechanism described here is only one of many inputs likely to be used by call-filtering algorithms operated by service providers, using data on calls from a particular identifier such as a telephone number to establish handling for future calls from the same identifier. Call handling for unwanted calls is likely to involve a combination of heuristics, analytics, and machine learning. These may use call characteristics such as call duration and call volumes for a particular caller, including changes in those metrics over time, as well as user feedback via non-SIP approaches and the mechanism described here. Implementations will have to make appropriate trade-offs between falsely labeling a caller as unwanted and delivering unwanted calls.

Systems receiving 607 responses could decide to treat pre-call and mid-call responses differently, given that the called party has had access to call content for mid-call rejections.

Depending on the implementation, the response code does not necessarily automatically block all calls from that caller identity. The same user interface action might also trigger addition of the caller identity to a local, on-device blacklist or graylist, e.g., causing such calls to be flagged or alerted with a different ring tone.

The actions described here do not depend on the nature of the SIP URI, e.g., whether or not it describes a telephone number; however, the same anonymous SIP URI [RFC3323] may be used by multiple callers; thus, such URIs are unlikely to be appropriate for URI-specific call treatment. SIP entities tallying responses for particular callers may need to consider canonicalzing SIP URIs, including telephone

numbers, as described in [SIP-IDENTITY]. The calling party may be identified in different locations in the SIP header, e.g., the From header field, P-Asserted-Identity or History-Info, and may also be affected by diverting services.

This document defines a SIP feature-capability [RFC6809], sip.607, that allows the registrar to indicate that the corresponding proxy supports this particular response code. This allows the UA, for example, to provide a suitable user-interface element, such as a "spam" button, only if its service provider actually supports the feature. The presence of the feature capability does not imply that the provider will take any particular action, such as blocking future calls. A UA may still decide to render a "spam" button even without such a capability if, for example, it maintains a device-local blacklist or reports unwanted calls to a third party.

5. IANA Considerations

5.1. SIP Response Code

This document registers a new SIP response code. This response code is defined by the following information, which has been added to the "Response Codes" subregistry under the "Session Initiation Protocol (SIP) Parameters" registry <http://www.iana.org/assignments/sip-parameters>.

Response Code: 607

Description: Unwanted

Reference: [RFC8197]

5.2. SIP Global Feature-Capability Indicator

This document defines the feature capability sip.607 in the "SIP Feature-Capability Indicator Registration Tree" registry defined in [RFC6809].

Name: sip.607

Description: This feature-capability indicator, when included in a Feature-Caps header field of a REGISTER response, indicates that the server supports, and will process, the 607 (Unwanted) response code.

Reference: [RFC8197]

6. Security Considerations

If the calling party address is spoofed, users may report the caller identity as placing unwanted calls, possibly leading to the blocking of calls from the legitimate user of the caller identity in addition to the unwanted caller, i.e., creating a form of denial-of-service attack. Thus, the response code SHOULD NOT be used for creating global call filters unless the calling party identity has been authenticated using [SIP-IDENTITY] as being assigned to the caller placing the unwanted call. (The creation of call filters local to a user agent is beyond the scope of this document.)

Even if the identity is not spoofed, a call or message recipient might flag legitimate caller identities, e.g., to exact vengeance on a person or business, or simply by mistake. To correct errors, any additions to a personal list of blocked caller identities should be observable and reversible by the party being protected by the blacklist. For example, the list may be shown on a web page or the subscriber may be notified by periodic email reminders. Any additions to a global or carrier-wide list of unwanted callers needs to consider that any user-initiated mechanism will suffer from an unavoidable rate of false positives and tailor their algorithms accordingly, e.g., by comparing the fraction of delivered calls for a particular caller that are flagged as unwanted rather than just the absolute number and considering time-weighted filters that give more credence to recent feedback.

If an attacker on an unsecured network can spoof SIP responses for a significant number of call recipients, it may be able to convince the call-filtering algorithm to block legitimate calls. Use of TLS to protect signaling mitigates against this risk.

Since caller identities are routinely reassigned to new subscribers, algorithms are advised to consider whether the caller identity has been reassigned to a new subscriber and possibly reset any related rating. (In some countries, there are services that track which telephone numbers have been disconnected before they are reassigned to a new subscriber.)

Some call services, such as 3PCC [RFC3725] and call transfer [RFC5359], increase the complexity of identifying who (if anyone) should be impacted by the receipt of 607 within BYE. Such services might cause the wrong party to be flagged or prevent flagging the desired party.

For both individually authenticated and unauthenticated calls, recipients of response code 607 may want to distinguish responses sent before and after the call has been answered, ascertaining whether either response timing suffers from a lower false-positive rate.

7. References

7.1. 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>.

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, DOI 10.17487/RFC3326, December 2002, <http://www.rfc-editor.org/info/rfc3326>.

[RFC6809] Holmberg, C., Sedlacek, I., and H. Kaplan, "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)", RFC 6809, DOI 10.17487/RFC6809, November 2012, <http://www.rfc-editor.org/info/rfc6809>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

7.2. 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>.

[RFC3725] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", BCP 85, RFC 3725, DOI 10.17487/RFC3725, April 2004, <http://www.rfc-editor.org/info/rfc3725>.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <http://www.rfc-editor.org/info/rfc3966>.

[RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", RFC 5039, DOI 10.17487/RFC5039, January 2008, <http://www.rfc-editor.org/info/rfc5039>.

[RFC5057] Sparks, R., "Multiple Dialog Usages in the Session Initiation Protocol", RFC 5057, DOI 10.17487/RFC5057, November 2007, <http://www.rfc-editor.org/info/rfc5057>.

[RFC5359] Johnston, A., Ed., Sparks, R., Cunningham, C., Donovan, S., and K. Summers, "Session Initiation Protocol Service Examples", BCP 144, RFC 5359, DOI 10.17487/RFC5359, October 2008, <http://www.rfc-editor.org/info/rfc5359>.

[SIP-IDENTITY] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", Work in Progress, draft-ietf-stir-rfc4474bis-16, February 2017.

Acknowledgements

Tolga Asveren, Ben Campbell, Peter Dawes, Spencer Dawkins, Martin Dolly, Keith Drage, Vijay Gurbani, Christer Holmberg, Olle Johansson, Paul Kyzivat, Jean Mahoney, Marianne Mohali, Adam Montville, Al Morton, Denis Ovsienko, Brian Rosen, Brett Tate, Chris Wendt, Dale Worley, and Peter Yee (Gen-ART reviewer) provided helpful comments.

Author’s Address

Henning Schulzrinne
FCC
445 12th Street SW
Washington, DC 20554
United States of America

Email: henning.schulzrinne@fcc.gov