Network Working Group
Request for Comments: 4453
Category: Informational

J. Rosenberg
Cisco Systems
G. Camarillo, Ed.
Ericsson
D. Willis
Cisco Systems

April 2006

# Requirements for Consent-Based Communications in the Session Initiation Protocol (SIP)

## Status of This Memo



## Copyright Notice



## Abstract

The Session Initiation Protocol (SIP) supports communications across many media types, including real-time audio, video, text, instant messaging, and presence. In its current form, it allows session invitations, instant messages, and other requests to be delivered from one party to another without requiring explicit consent of the recipient. Without such consent, it is possible for SIP to be used for malicious purposes, including spam and denial-of-service attacks. This document identifies a set of requirements for extensions to SIP that add consent-based communications.

## Table of Contents

## 1. Introduction

The Session Initiation Protocol (SIP) [1] supports communications across many media types, including real-time audio, video, text, instant messaging, and presence. This communication is established by the transmission of various SIP requests (such as INVITE and MESSAGE [3]) from an initiator to the recipient, with whom communication is desired. Although a recipient of such a SIP request can reject the request, and therefore decline the session, a SIP network will deliver a SIP request to the recipient without their explicit consent.

Receipt of these requests without explicit consent can cause a number of problems in SIP networks. These include amplification attacks. These problems have plagued email. At the time of this writing, most SIP services are not interconnected, so the incidence of amplification attacks directed at SIP services is low compared to the same attacks on email services. The SIPPING working group believes it is necessary to address these attacks proactively so the attacks do not become as burdensome as attacks on email have become.

This document elaborates on the problems posed by the current open model in which SIP was designed, and then goes on to define a set of requirements for adding a consent framework to SIP.

## 2. Problem Statement

In SIP networks designed according to the principles of RFC 3261 [1] and RFC 3263 [2], anyone on the Internet can create and send a SIP request to any other SIP user, by identifying that user with a SIP Uniform Resource Identifier (URI). The SIP network will usually deliver this request to the user identified by that URI. It is possible, of course, for network services, such as call screening, to block such messaging from occurring, but this is not widespread and certainly not a systematic solution to the problem under consideration here.

Once the SIP request is received by the recipient, the user agent typically takes some kind of automated action to alert the user about receipt of the message. For INVITE requests, this usually involves delivering an audible alert (e.g., "ringing the phone"), or a visual alert (e.g., creating a screen pop-up window). These indicators frequently convey the subject of the call and the identity of the caller. Due to the real-time nature of the session, these alerts are typically disruptive in nature, so as to get the attention of the user.

For MESSAGE requests, the content of the message is usually rendered to the user.

SUBSCRIBE [4] requests do not normally get delivered to the user agents residing on a user's devices. Rather, they are normally processed by network-based state agents. The watcher information event package allows a user to find out that such requests were generated for them, affording the user the opportunity to approve or deny the request. As a result, SUBSCRIBE processing, and most notably presence, already has a consent-based operation. Nevertheless, this already-existing consent mechanism for SIP subscriptions does not protect network agents against denial-of-service (DoS) attacks.

A problem that arises when requests can be delivered to user agents directly, without their consent, is amplification attacks. SIP proxies provide a convenient relay point for targeting a message to a particular user or IP address and, in particular, forwarding to a recipient that is often not directly reachable without usage of the proxy. Some SIP proxy servers forward a single request to several instances or contacts for the same user or resource. This process is called "forking". Another type of SIP server provides the SIP URI-list service [5], which sends a new copy of the same request to each recipient in the URI-list. Examples of URI-list services are subscriptions to resource lists [6], dial-out conference servers [8], and MESSAGE URI-list services [7]. A SIP URI-list service could be used as an amplifier, allowing a single SIP request to flood a single target host or network. For example, a user can create a resource list with 100 entries, each of which is a URI of the form "sip:identifier@target-IP", where target-IP is the IP address to which the attack is to be directed. Sending a single SIP SUBSCRIBE request to such a list will cause the resource list server to generate 100 SUBSCRIBE requests, each to the IP address of the target, which does not even need to be a SIP node.

> Note that the target-IP does not need to be the same in all the URIs in order to attack a single machine. For example, the target-IP addresses may all belong to the same subnetwork, in which case the target of the attack would be the access router of the subnetwork.

In addition to launching DoS attacks, attackers could also use SIP URI-list servers as amplifiers to deliver spam. For INVITE requests, this takes the form of typical "telemarketer" calls. A user might receive a stream of never-ending requests for communications, each of them disrupting the user and demanding their attention. For MESSAGE requests, the problem is even more severe. The user might receive a never-ending stream of visual alerts (e.g., screen pop-up windows) that deliver unwanted, malicious, or otherwise undesired content.

Both amplification attacks related to spam and DoS can be alleviated by adding a consent-based communications framework to SIP. Such a framework keeps servers from relaying messages to users without their consent.

> The framework for SIP URI-list services [5] identifies amplification attacks as a problem in the context of URI-list services. That framework mandates the use of opt-in lists, which are a form of consent-based communications. The reader can find an analysis on how a consent-based framework helps alleviate spam-related problems in [9].

## 3. Requirements

The following identify requirements for a solution that provides consent-based communications in SIP. A relay is defined as any SIP server, be it a proxy, Back-to-Back User Agent (B2BUA), or some hybrid, that receives a request and translates the request URI into one or more next-hop URIs to which it then delivers a request.

REQ 1: The solution must keep relays from delivering a SIP request to a recipient unless the recipient has explicitly granted permission to the relay using appropriately authenticated messages.

REQ 2: The solution shall prevent relays from generating more than one outbound request in response to an inbound request, unless permission to do so has been granted by the resource to whom the outbound request was to be targeted. This requirement avoids the consent mechanism itself becoming the focus of DoS attacks.

REQ 3: The permissions shall be capable of specifying that messages from a specific user, identified by a SIP URI that is an Address-of-Record (AOR), are permitted.

REQ 4: Each recipient AOR must be able to specify permissions separately for each SIP service that forwards messages to the recipient. For example, Alice may authorize forwarding to her from domain A, but not from domain B.

REQ 5: It shall be possible for a user to revoke permissions at any time.

REQ 6: It shall not be required for a user or user agent to store information in order to be able to revoke permissions that were previously granted for a relay resource.

REQ 7: The solution shall work in an inter-domain context, without requiring preestablished relationships between domains.

REQ 8: The solution shall work for all current and future SIP methods.

REQ 9: The solution shall be applicable to forking proxies.

REQ 10: The solution shall be applicable to URI-list services, such as resource list servers [5], MESSAGE URI-list services [7], and conference servers performing dial-out functions [8].

REQ 11: In SIP, URI-lists can be stored on the URI-list server or provided in a SIP request. The consent framework must work in both cases.

REQ 12: The solution shall allow anonymous communications, as long as the recipient is willing to accept anonymous communications.

REQ 13: If the recipient of a request wishes to be anonymous with respect to the original sender, it must be possible for the recipient to grant permission for the sender without the original sender learning the recipient's identity.

REQ 14: The solution shall prevent attacks that seek to undermine the underlying goal of consent. That is, it should not be possible to "fool" the system into delivering a request for which permission was not, in fact, granted.

REQ 15: The solution shall not require the recipient of the communications to be connected to the network at the time communications are attempted.

REQ 16: The solution shall not require the sender of a SIP request to be connected at the time that a recipient provides permission.

REQ 17: The solution should scale to Internet-wide deployment.

# 4. Security Considerations

Security has been discussed throughout this document.

## 5. References

### 5.1. 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] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[3] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

### 5.2. Informational References

[4] Roach, A.B., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[5] Camarillo, G. and A.B. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)-List Services", Work in Progress, January 2006.

[6] Roach, A.B., Rosenberg, J., and B. Campbell, "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", Work in Progress, January 2005.

[7] Garcia-Martin, M. and G. Camarillo, "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)", Work in Progress, February 2006.

[8] Camarillo, G. and A. Johnston, "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)", Work in Progress, February 2006.

[9] Rosenberg, J., "The Session Initiation Protocol (SIP) and Spam", Work in Progress, July 2005.

## Authors' Addresses

Jonathan Rosenberg
Cisco Systems
600 Lanidex Plaza
Parsippany, NJ 07054
US

Phone: +1 973 952-5000
EMail: jdrosen@cisco.com
URI: http://www.jdrosen.net

Gonzalo Camarillo (Editor)
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com

Dean Willis
Cisco Systems
2200 E. Pres. George Bush Turnpike
Richardson, TX 75082
USA

EMail: dean.willis@softarmor.com

## Acknowledgement

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