SIP
Internet-Draft
Expires: January 6, 2005

J. Rosenberg
dynamicsoft
G. Camarillo
Ericsson
D. Willis
dynamicsoft

July 8, 2004

Requirements for Consent-Based Communications in the Session Initiation Protocol (SIP)
draft-rosenberg-sipping-consent-reqs-00.txt

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 [4]) 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 spam and DoS (Denial of Service) attacks. These problems have plagued email. Fortunately, most SIP networks, at time of writing, were not interconnected with each other, and so the incidences of such problems have been lower. However, once such broad interconnection occurs, these problems will arise. Therefore, it is important to address them proactively, before it is too late.

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 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 occuring, 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 "ringing the phone", or creating a screen pop. 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 [3] 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 DoS attacks.

There are two principal problems that arise when MESSAGE and INVITE requests can be delivered to user agents directly, without their consent. The first is 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 screen pops that deliver unwanted, malicious, or otherwise undesired content.

The second problem is DoS attacks. SIP proxies provide a convenient relay point for targeting a message to a particular user or IP address, and in particular, relaying to a recipient which is often not directly reachable without usage of the proxy. Worse, some proxies or back to back user agents generate multiple outgoing requests upon receipt of an incoming request. This occurs in forking proxies, and in URI-list services. Examples of URI-list services are subscriptions to resource lists, dial out conference servers, and

MESSAGE URI-list services. These SIP elements can be used as an amplifier, allowing the transmission of a single SIP request to flood packets to a single recipient or network. For example, a user can create a buddy 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.

Though the spam and DoS problems are not quite the same, both 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 [draft-ietf-sipping-uri-services-00.txt] identifies these two problems (spam and DoS attacks) 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 help alleviating spam-related problems in [draft-rosenberg-sipping-spam-00.txt]

3. Requirements

The following identify requirements for a solution that provides consent-based communications in SIP.

REQ 1: The solution must keep relays from delivering a SIP message to a recipient unless the recipient has explicitly granted permission for receipt of that type of message.

REQ 2: The solution shall prevent SIP servers 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.

REQ 3: The permissions shall be capable of specifying that messages from a specific user, identified by a SIP AoR, are permitted.

REQ 4: It shall be possible for a user with a particular AoR to specify permissions separately for each resource that wishes to relay requests to that AOR.

REQ 5: The permissions shall be capable of specifying that only certain types of messages, such as INVITE or MESSAGE request, are permitted from a user.

REQ 6: It shall be possible for a user to revoke permissions at any time.

REQ 7: It shall be possible for the users to specify that permissions are time limited, and must be refreshed after expiration.

REQ 8: 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 9: The solution shall work in an inter-domain context, without requiring pre-established relationships between domains.

REQ 10: The solution shall work for all current and future SIP methods.

REQ 11: The solution shall be applicable to forking proxies.

REQ 12: The solution shall be applicable to URI-list services, such as resource list servers, MESSAGE URI-list services, and conference servers performing dial-out functions.

REQ 13: The solution shall be applicable to both stored and request-contained URI-list services.

REQ 14: The solution shall allow anonymous communications, as long as

the recipient is willing to accept anonymous communications.

REQ 15: If the recipient of requests wishes to be anonymous, it shall be possible for them to grant permissions without a sender knowing their identity.

REQ 16: The solution shall prevent against 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 17: The solution shall not require the recipient of the communications to be connected to the network at the time communications is attempted.

REQ 18: The solution shall note require the sender of a communications to be connected at the time that a recipient provides permission.

REQ 19: The solution should not, in and of itself, create substantial additional messaging. Doing so defeats some of the purpose of the solution.

REQ 20: The solution should scale to Internet-wide deployment.

4. Security Considerations

Security has been discussed throughout this specification.

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

[4] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C. and D.

Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

Authors' Addresses

Jonathan Rosenberg
dynamicsoft
600 Lanidex Plaza
Parsippany, NJ 07054
US

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

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com

Dean Willis
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, TX 75028
USA

EMail: dean.willis@softarmor.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.