Internet Engineering Task Force R. Sparks
Internet Draft MCI WorldCom
draft-sparks-sip-multiproxy-auth-00.txt
October 1999
Expires: April 2000

# Providing for Multiple-Proxy Authentication of a SIP Request

STATUS OF THIS MEMO



Abstract

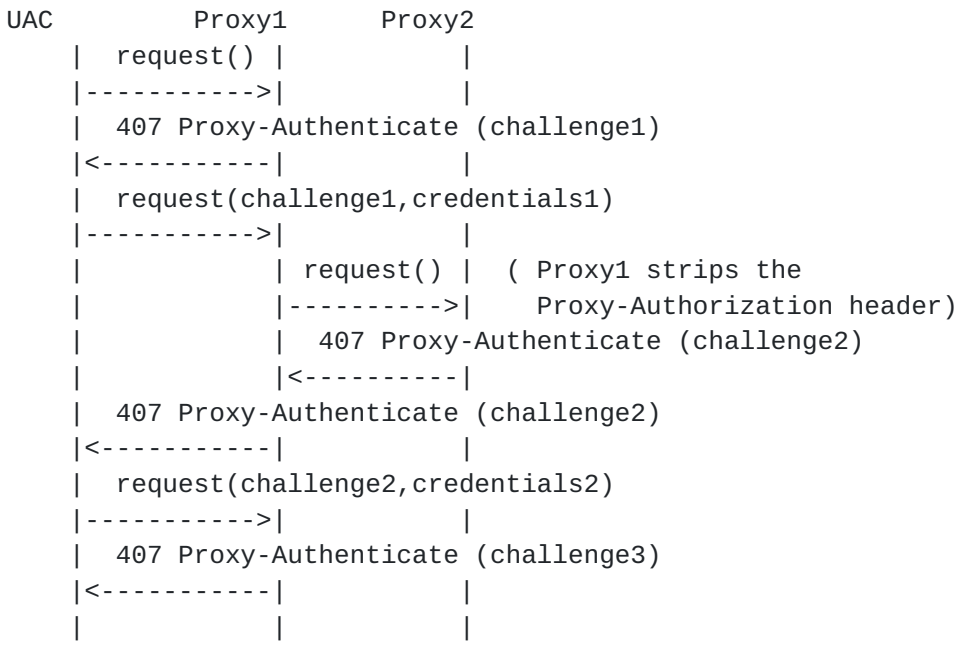
SIP/2.0 as specified in RFC2543 provides a mechanism for a proxy involved in a SIP transaction to authenticate the originator of the request. Unfortunately, this mechanism is not well defined when more than one proxy in a requestÆs path desires such authentication. This draft proposes a mechanism that would allow authentication in that scenario to work as expected. Under this proposal, SIP clients would issue requests with multiple Proxy-Authorization headers, one for each challenge it has seen in the lifetime of a given call leg. Authenticating SIP proxies would search each request for a Proxy-Authorization response to its own challenge, passing any others downstream unaltered.

## Introduction

A request from a SIP client may pass through several proxies before reaching its intended destination. Any of these proxies may require authenticating credentials from an upstream proxy, or the source of the request, before passing the request along. Section 6.2 of the RFC2543 [1] reuses the definition and recommended behavior for Proxy-Authorization from HTTP:

> "The Proxy-Authorization request-header field allows the client to identify itself (or its user) to a proxy which requires authentication. The Proxy-Authorization field value consists of credentials containing the authentication information of the user agent for the proxy and/or realm of the resource being requested.
> Unlike Authorization, the Proxy-Authorization header field applies only to the next outbound proxy that demanded authentication using the Proxy-Authenticate field. When multiple proxies are used in a chain, the Proxy-Authorization header field is consumed by the first outbound proxy that was expecting to receive credentials. A proxy MAY relay the credentials from the client request to the next proxy if that is the mechanism by which the proxies cooperatively authenticate a given request."

By itself, this definition allows for unexpected behavior when more than one proxy in the request path desires authentication. Consider the following scenario (each message label is associated with the arrow immediately below it):



Here, Proxy1 did not recognize the response to Proxy2Æs challenge, so it challenges again.

Proposal

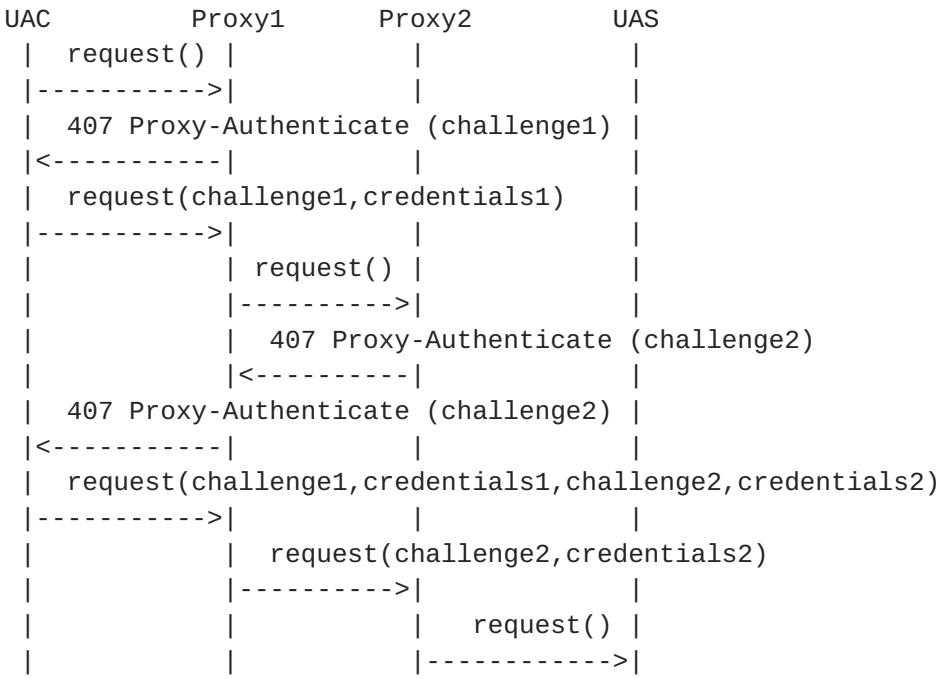
To avoid this type of failure, the following extensions to the behavior specified in RFC2543 are proposed.

1) For the duration of a call-leg (To:,From:,Call-ID), a UAC will retain any proxy challenge material received and include a response to each challenge in a separate Proxy-Authorization header in each subsequent request in that call-leg. While retaining challenge material, a UAC must be sensitive to the realm of the request, so that stale challenges are replaced with their updates.

2) Any proxy requiring authentication that receives a request with multiple Proxy-Authenticate headers will search for headers with challenge parameters matching those it requested. If no such header is found, the proxy will reply with a challenge. If exactly one such header is found, the proxy will verify the credentials and forward the message or issue a challenge/failure. If more than one such header is found, the proxy will reply with a 403 Forbidden (to discourage hunting for valid credentials).

3) A proxy not requiring authentication or a proxy whose challenge has been satisfied will forward all other Proxy-Authentication headers downstream unaltered. A proxy MAY remove the Proxy-Authentication header that was meant for it.

Under this proposal, the above scenario would play out as follows:




A UAC should be prepared to terminate the deadlock situation caused

by a proxy in the chain that expires a challenge after its first successful response. Proxies implementing this proposal must accept a valid response to a challenge more than once within the context of a given call-leg. Multiple proxies in the same administrative domain must take care to issue unique realm strings.

Acknowledgments

The author would like to thank the following for their discussion of and contribution to this work:

Matt Cannon
Chris Cunningham
Steve Donovan
Alan Johnston
Henry Sinnreich
John Truetken
Dean Willis

AuthorÆs Address

Robert Sparks
MCI WorldCom
9137/107
2400 N. Glenville Road
Richardson, Texas 75082
email: robert.sparks@wcom.com

Bibliography

[1] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol", Request for Comments (Proposed Standard) 2543, Internet Engineering Task Force, Mar. 1999.