SIPCORE Working Group
INTERNET-DRAFT
Intended Status: Standards Track
Expires: July 21, 2014

R. Shekh-Yusef
Avaya

January 17, 2014

The Session Initiation Protocol (SIP) Digest Authentication Scheme
draft-yusef-sipcore-digest-scheme-02

Abstract

This document updates the Digest Access Authentication scheme used by the Session Initiation Protocol (SIP) to add support for SHA2 digest algorithms to replace the MD5 algorithm.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Table of Contents

1 Introduction

The SIP protocol [RFC3261] uses the same mechanism used by the HTTP protocol for authenticating users, which is a simple challenge-response authentication mechanism that allows a server to challenge a client request and allows a client to provide authentication information in response to that challenge.

The SIP protocol uses the Digest Authentication scheme that is used with the HTTP authentication mechanism, which by default uses MD5 as the default algorithm.

The HTTP Digest Access Authentication [HTTP-DIGEST] document defines the challenge-response authentication mechanism and the Digest Authentication scheme, and defines few algorithms that could be used with the Digest Authentication scheme, and establishes a registry for these algorithms to allow for additional algorithms to be added in the future.

In 2008 the US-CERT issued a note that MD5 "should be considered cryptographically broken and unsuitable for further use" [CERT-VU].

This document updates the Digest Access Authentication scheme used by SIP to add support for SHA2 digest algorithms to replace the MD5 algorithm.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2 The SIP Digest Authentication Scheme

This section describes the modifications to the operation of the Digest mechanism as specified in RFC3261.

2.1 Hash Algorithms

The Digest scheme has an 'algorithm' parameter that specifies the algorithm to be used to compute the digest of the response.

RFC3261 specifies only one algorithm, MD5, which is used by default. This document adds two new algorithms, to align with the [HTTP-DIGEST], that SHOULD be used instead of MD5: SHA2-256 & SHA2-512/256.

This document defines the following preference list, starting with the most preferred algorithm:

* SHA2-256 (most preferred)
* SHA2-512/256
* MD5 (least preferred)

2.2 Representation of Digest Values

The size of the digest depends on the algorithm used. The bits in the digest are converted from the most significant to the least significant bit, four bits at a time to the ASCII representation as follows. Each four bits is represented by its familiar hexadecimal notation from the characters 0123456789abcdef, that is binary 0000 is represented by the character '0', 0001 by '1' and so on up to the representation of 1111 as 'f'. If the MD5 algorithm is used to calculate the digest, then the digest will be represented as 32 hexadecimal characters, SHA2-256 and SHA2-512/256 by 64 hexadecimal characters.

2.3 The Authenticate Response Header

When a UAS receives a request from a UAC, and an acceptable Authorization header is not sent, the UAS can challenge the originator to provide credentials by rejecting the request with a 401/407 status code with the WWW-Authenticate/Proxy-Authenticate header field. The UAS MAY include multiple WWW-Authenticate/Proxy-Authenticate headers to allow the UAS to utilize the best available algorithm supported by the client.

If the UAS challenges with multiple WWW-Authenticate/Proxy-

Authenticate headers, then each one of these headers MUST use a different digest algorithm. The UAS MUST add these headers to the response in order of strength of the algorithm, starting with the strongest algorithm, followed by the less strong algorithms.

2.4 The Authorization Request Header

When the UAC receives the response it SHOULD use the topmost header that it supports, unless a local policy dictates otherwise. The client should ignore any challenge it does not understand.

If the UAC does not support any of the algorithms in the response, then it should abandon attempts to send the request.

2.5 Forking

RFC3261, section 22.3, discusses the operation of the proxy-to-user authentication, which describes the operation of the proxy when it forks a request. This section introduces some clarification to that operation.

If a request is forked, various proxy servers and/or UAs may wish to challenge the UAC. In this case, the forking proxy server is responsible for aggregating these challenges into a single response. Each WWW-Authenticate and Proxy-Authenticate value received in responses to the forked request MUST be placed into the single response that is sent by the forking proxy to the UA.

When the forking proxy places multiple WWW-Authenticate and Proxy-Authenticate header fields from one proxy into the single response it MUST maintain the order of these header fields. The ordering of the header field values from the various proxies is not significant.

2.6 HTTP Modifications

This section describes the modifications and clarifications required to apply the HTTP Digest authentication scheme to SIP. The SIP scheme usage is almost completely identical to that for HTTP.

SIP clients and servers MUST NOT accept or request Basic authentication.

The rules for Digest authentication follow those defined in HTTP, with "HTTP/1.1" replaced by "SIP/2.0" in addition to the following differences:

1. The URI included in the challenge has the following BNF:

   URI = SIP-URI / SIPS-URI

2. The BNF for digest-uri-value is:

   digest-uri-value = Request-URI ; as defined in Section 25

3. The example procedure for choosing a nonce based on Etag does not work for SIP.

4. The text in RFC 2617 [17] regarding cache operation does not apply to SIP.

5. RFC 2617 requires that a server check that the URI in the request line and the URI included in the Authorization header field point to the same resource. In a SIP context, these two URIs may refer to different users, due to forwarding at some proxy. Therefore, in SIP, a server MAY check that the Request-URI in the Authorization header field value corresponds to a user for whom the server is willing to accept forwarded or direct requests, but it is not necessarily a failure if the two fields are not equivalent.

6. As a clarification to the calculation of the A2 value for message integrity assurance in the Digest authentication scheme, implementers should assume, when the entity-body is empty (that is, when SIP messages have no body) that the hash of the entity-body resolves to the hash of an empty string, or:

   H(entity-body) = MD5("") =
   "d41d8cd98f00b204e9800998ecf8427e"

   H(entity-body) = SHA2-256("") =
   "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"

   H(entity-body) = SHA2-512-256("") =
   "c672b8d1ef56ed28ab87c3622c5114069bdd3ad7b8f9737498d0c01ecef0967a"

7. Servers MUST be able to properly handle "qop" parameter received in an authorization header field, and clients MUST be able to properly handle "qop" parameter received in WWW-Authenticate and Proxy-Authenticate header fields.

   Servers MUST always send a "qop" parameter in WWW-Authenticate and Proxy-Authenticate header field values, and clients MUST send the "qop" parameter in any resulting authorization header field.

The usage of the Authentication-Info header field continue to be allowed, since it provides integrity checks over the bodies and provides mutual authentication.

[OPEN ISSUE]

This section does NOT maintain backward compatibility with RFC 2543.

3 Augmented BNF for the SIP Protocol

This document updates the Augmented BNF for the SIP Protocol as follows.

It extends the request-digest as follows to allow for different digest sizes:

```
request-digest    =  LDQUOT 32LHEX RDQUOT / LDQUOT 64LHEX RDQUOT
```

It extends the algorithm parameter as follows to allow for SHA2 algorithms to be used:

```
algorithm =  "algorithm" EQUAL (
                          "MD5" / "MD5-sess" /
                          "SHA2-256" / "SHA2-256-sess" /
                          "SHA2-512-256" / "SHA2-512-256-sess" /
                          token )
```

4 Security Considerations

<Security considerations text>

5 IANA Considerations

The [HTTP-DIGEST] defines an IANA registry named "HTTP Digest Hash Algorithms" to simplify the introduction of new algorithms in the future. This document will use the algorithms defined in that registry.

6 Acknowledgments

<Acknowledgments text>

7 References

7.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[HTTP-DIGEST] Shekh-Yusef, R., Ahrens, D., and Bremer, S., "HTTP Digest Access Authentication", Work in Progress, January 2014.

https://datatracker.ietf.org/doc/draft-ietf-httpauth-digest/

7.2 Informative References

Authors' Addresses

Rifaat Shekh-Yusef
Avaya
250 Sydney Street
Belleville, Ontario
Canada

Phone: +1-613-967-5267
Email: rifaat.ietf@gmail.com