SIPCORE Working Group
INTERNET-DRAFT
Intended Status: Standards Track
Expires: July 14, 2014

R. Shekh-Yusef
Avaya

January 10, 2014

The Session Initiation Protocol (SIP) Digest Authentication Scheme
draft-yusef-sipcore-digest-scheme-00

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

Copyright and License Notice

Table of Contents

1 Introduction 3
1.1 Terminology 3
2 The SIP Digest Authentication Scheme 3
3 Augmented BNF for the SIP Protocol 6
4 Security Considerations 6
5 IANA Considerations 6
6 Acknowledgments 6
7 References 7
7.1 Normative References 7
7.2 Informative References 7
Authors' Addresses 7

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.

This document replaces what is specified in RFC3261, Section 22.4.

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 document 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 [HTTP-DIGEST].

Since RFC 2543 is based on HTTP Digest as defined in RFC 2069, SIP servers supporting [HTTP-DIGEST] MUST ensure they are backwards compatible with RFC 2069. Procedures for this backwards compatibility are specified in [HTTP-DIGEST]. Note, however, that SIP servers MUST NOT accept or request Basic authentication.

The rules for Digest authentication follow those defined in [HTTP-DIGEST], 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
   ```

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

4. The text in [HTTP-DIGEST] regarding cache operation does not apply to SIP.

5. [HTTP-DIGEST] 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 as follows:

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

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

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

"TODO"

7. [HTTP-DIGEST] notes that a cnonce value MUST NOT be sent in an Authorization (and by extension Proxy-Authorization) header field if no qop directive has been sent. Therefore, any algorithms that have a dependency on the cnonce (including "MD5-sess", "SHA2-256-sess", and "SHA2-512-256-sess") require that the qop directive be sent. Use of the "qop" parameter is optional in [HTTP-DIGEST] for the purposes of backwards compatibility with RFC 2069; since RFC 2543 was based on RFC 2069, the "qop" parameter must unfortunately remain optional for clients and servers to receive. However, servers MUST always send a "qop" parameter in WWW-Authenticate and Proxy-Authenticate header field values. If a client receives a "qop" parameter in a challenge header field, it MUST send the "qop" parameter in any resulting authorization header field.

RFC 2543 did not allow usage of the Authentication-Info header field (it effectively used RFC 2069). However, we now allow usage of this header field, since it provides integrity checks over the bodies and provides mutual authentication. [HTTP-DIGEST] defines mechanisms for backwards compatibility using the qop attribute in the request. These mechanisms MUST be used by a server to determine if the client supports the new mechanisms in [HTTP-DIGEST] that were not specified in RFC 2069.

[OPEN ISSUE:]

Should the backward compatibility with RFC2543/RFC2069 be deprecated?

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 digest-size LHEX RDQUOT
digest-size       = "32" / "64"
```

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

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

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