Network Working Group
Internet-Draft
Intended status: Standards Track
Obsoletes: 2747 (if approved)
Expires: October 19, 2013

S. Turner, Ed.
IECA
L. Berger
LabN Consulting
M. Jethanandani
Ciena
K. Patel
Cisco Systems
D. Zhang
Huawei

April 17, 2013

Cryptographic Agility for the RSVP INTEGRITY Object
draft-turner-rsvp-auth-update-00

Abstract

This document modifies the RSVP INTEGRITY object to support algorithm agility by explicitly indicating the algorithm used. It also provides rationale for the design choices. Finally, it updates the mandatory to implement algorithm.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

1. Introduction

RSVP Cryptographic Authentication, defined in [RFC2747] and updated [RFC3097], defines the INTEGRITY object format to enable RSVP message integrity on a hop-by-hop basis. It also specifies the MTI (mandatory to implement) algorithm, HMAC-MD5 [RFC2104].

The integrity algorithm used is not indicated in the INTEGRITY object and is therefore either negotiated via another mechanism or manually configured. Lacking a negotiation mechanism essentially means the algorithm is hard coded. Hard coding algorithms once fashionable is no longer de riqueur. Instead, protocols needs to support algorithm agility because cryptographic protocols weaken over time as cryptanalysis against them improves. This document provides a cryptographically agile INTEGRITY object and it also provides rationale for the choices.

Spoiler Alert: The change is to use the unused fields between the Flags and Key Identifier fields to indicate the integrity algorithm.

This document does not change the authentication mechanism (i.e., it's still HMAC-based authentication), but it does change the mandatory to implement algorithm.

2. Terminology

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

Familiarity with [RFC2747] is assumed.

3. Design Methodology

This section is informative. It may or may not be removed in the final version.

HMAC-MD5 may not yet be inappropriate to use [RFC6151], but RSVP needs to support algorithm agility in case HMAC-MD5 ever does become insecure.

The solution proposed in s3.2 proposed to reuse the Class Number 4 instead of defining another Class Number for an INTEGRITYv2 object. In order to do this, the algorithm choice needs to be carried in the object itself. Options exist:

- Use one or more of the unused Flags fields. A 7-bit fields would allow 127 additional algorithms to be specified, with 0 indicating the existing algorithm.

- Use the unused byte between the Flags and the Key Identifier. This would allow an additional 255 algorithms to be specified.

- Use a special value in one Key Identifier, Sequence Number of Keyed Message Digest and add another field. This would allow an almost infinite number of algorithms to be specified.

Luckily, there's no requirement to support an infinite number of algorithms and besides disrupting the order of the fields seems like too much of an implementation burden.

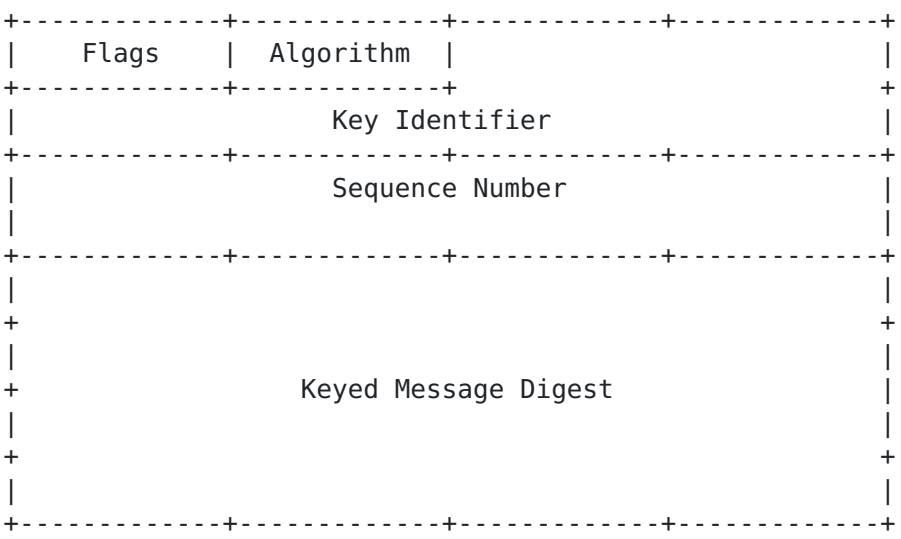
Co-opting some of the unused bits seems best. Flags seem more generic and it would be better to not take them all up. Therefore, using the byte between the Flags and Key Identifier was chosen.

4. Cryptographically Agile INTEGRITY Object

The same INTEGRITY object type is used for both IPv4 and IPv6.

The INTEGRITY object has the following format:

Keyed Message Digest INTEGRITY Object: Class = 4, C-Type = 1



The Flags, Key Identifier, Sequence Number, and Keyed Message Digest fields are as defined in [RFC2747].

Algorithm indicates the integrity algorithm used.

5. Mandatory to Implement Algorithm

[RFC2747] mandates support for HMAC-MD5. This document specifies the mandatory to implement algorithm as HMAC-SHA256 [RFC2104][SHS].

6. IANA Considerations

This document establishes a new sub-registry to the RSVP Class Types 4 C-Types 1 INTEGRITY registry for integrity algorithms. The assignment policy is Specification Required [RFC5226]. The initial table is as follows:

Alg Flag	Algorithm Name	Keyed Digest Size (bytes)
0	HMAC-MD5	16
1	HMAC-SHA1	20
1	HMAC-SHA224	28
3	HMAC-SHA224	32
4	HMAC-SHA384	48
5	HMAC-SHA512	64

7. Security Considerations

TBD

8. References

8.1. Normative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

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

[RFC2747] Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.

[RFC3097] Braden, R. and L. Zhang, "RSVP Cryptographic Authentication -- Updated Message Type Value", RFC 3097, April 2001.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[SHS] National Institute of Standards and Technology (NIST), FIPS Publication 186-3: Digital Signature Standard, October 2008.

8.2. Informative References

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

Authors' Addresses

Lou Berger
LabN Consulting L.L.C.

Phone: +1-301-468-9228
EMail: lberger@labn.net

Mahesh Jethanandani
Ciena Corporation
1741 Technology Drive
San Jose, CA 95110
USA

Phone: +1 (408) 436-3313
Email: mjethanandani@gmail.com

Keyur Patel
Cisco Systems Inc.
170 West Tasman Dr
San Jose, CA 95134
US

Email: keyupate@cisco.com

Sean Turner (editor)
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, Virginia 22031
US

Phone: +1 (703) 628-3180
Email: turners@ieca.com

Dacheng Zhang
Huawei Technologies Co., LTD.
Beijing,
China

Email: zhangdacheng@huawei.com