Vendor Specific RADIUS Attributes for the Delivery of Keying Material
draft-zorn-radius-keywrap-16.txt

Abstract

This document defines a set of vendor specific RADIUS Attributes designed to allow both the secure transmission of cryptographic keying material and strong authentication of any RADIUS message.

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."

This Internet-Draft will expire on January 10, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction .................................................. 3
2. Specification of Requirements ................................. 3
3. Attributes ....................................................... 3
   3.1. Keying-Material ......................................... 4
   3.2. MAC-Randomizer ......................................... 9
   3.3. Message-Authentication-Code .............................. 10
4. IANA Considerations ........................................... 15
5. Security Considerations ...................................... 15
6. Contributors ................................................... 16
7. Acknowledgements .............................................. 16
8. References ..................................................... 16
   8.1. Normative References .................................... 16
   8.2. Informative References ................................. 17
Authors’ Addresses .............................................. 17
1. Introduction

Many remote access deployments (for example, deployments utilizing wireless LAN technology) require the secure transmission of cryptographic keying material from a RADIUS [RFC2865] server to a network access point. Typically, this material is produced as a byproduct of an EAP [RFC3748] authentication and is of a form that may be used in virtually any cryptographic algorithm after appropriate processing.

This document defines a set of vendor specific RADIUS Attributes that can be used to securely transfer cryptographic keying material using standard techniques with well understood security properties. In addition, the Message-Authentication-Code Attribute may be used to provide strong authentication for any RADIUS message, including those used for accounting and dynamic authorization.

Discussion of this draft may be directed to the authors.

2. Specification of Requirements

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 [RFC2119].

3. Attributes

The following subsections describe sub-attributes which are transmitted in one or more RADIUS attributes of type Vendor-Specific [RFC2865]. The Vendor-ID field of the Vendor-Specific Attribute(s) MUST be set to decimal 9 (Cisco). The general format of the attributes is:

```
  0                   1                   2                   3
  +---------------+---------------+---------------+---------------+
  |     Type (26)  |    Length    | Vendor ID    |
  +---------------+---------------+---------------+
  | Vendor ID (cont’d) | Sub-type (1) | Sub-length |
  +---------------+---------------+---------------+
  |                     Value...
  +---------------+---------------+---------------+
```
Type

26 for vendor specific

Length

Length of entire attribute including type and length field

Vendor ID

4 octets encoding the Cisco Vendor ID of 9

Sub-type

Attribute sub-type of 1

Sub-length

Length of the sub attribute including the sub-type and sub-length fields

Value

Value of the sub attribute.

This specification concerns the following sub-attributes:

- Keying-Material
- MAC-Randomizer
- Message-Authentication-Code

3.1. Keying-Material

Description

This Attribute MAY be used to transfer cryptographic keying material from a RADIUS server to a client.

It MAY be sent in request messages (e.g., Access-Request, etc.), as well; if the Keying-Material Attribute is present in a request, it SHOULD be taken as a hint by the server that the client prefers this method of key delivery over others, the server is not obligated to honor the hint, however. When the Keying-Material Attribute is included in a request message the Key ID, Lifetime,
IV and Key Material fields MAY be omitted.

If the client requires the use of the Keying-Material Attribute for keying material delivery and it is not present in the Access-Accept or Access-Challenge message, the client MAY ignore the message in question and end the user session.

Any packet that contains a Keying-Material Attribute MUST also include the Message-Authentication-Code Attribute.

Any packet that contains an instance of the Keying-Material Attribute MUST NOT contain an instance of any other attribute (e.g., MS-CHAP-MPPE-Keys [RFC2548], Tunnel-Password [RFC2868], etc.) encapsulating identical keying material.

The Keying-Material Attribute MUST NOT be used to transfer long-lived keys (i.e., passwords) between RADIUS servers and clients.

A summary of the Keying-Material attribute format is shown below. The fields are transmitted from left to right.
<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type (26)</td>
<td>Length</td>
<td>Vendor ID</td>
<td></td>
</tr>
<tr>
<td>Vendor ID (cont’d)</td>
<td>Sub-type (1)</td>
<td>Sub-length</td>
<td></td>
</tr>
<tr>
<td>String ID (&quot;radius:app-key=&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>String ID (cont’d)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Type**

26 for vendor specific
Length
Length of entire attribute including type and length field

Vendor ID
4 octets encoding the Cisco Vendor ID of 9

Sub-type
Attribute sub-type of 1

Sub-length
Length of the sub attribute including the sub-type and sub-length fields

String-ID
The ASCII characters "radius:app-key=" without quotes or null termination.

Enc Type
The Enc Type field indicates the method used to encrypt the contents of the Data field. This document defines only one value (decimal) for this field:

0 AES Key Wrap with 128-bit KEK [RFC3394]

Implementations MUST support Enc Type 0 (AES Key Wrap with 128-bit KEK).

Implementation Note

A shared secret is used as the key-encrypting-key (KEK) for the AES key wrap algorithm. Implementations SHOULD provide a means to provision a key (cryptographically separate from the normal RADIUS shared secret) to be used exclusively as a KEK.

App ID

The App ID field is 4 octets in length and identifies the type of application for which the key material is to be used. This allows for multiple keys for different purposes to be present in the same message. This document defines two values for the App ID:
0 Unspecified
1 EAP MSK

Further specification of the content of this field is outside the scope of this document.

KEK ID

The KEK ID field is 16 octets in length and contains an identifier for the KEK. The KEK ID MUST refer to an encryption key of a type and length appropriate for use with the algorithm specified by the Enc Type field (see above). This key is used to protect the contents of the Data field (below). Further specification of the content of this field is outside the scope of this document.

KM ID

The KM ID field is 16 octets in length and contains an identifier for the contents of the Data field. The KM ID MAY be used by communicating parties to identify the material being transmitted. The combination of App ID and KM ID MUST uniquely identify the keying material between the parties utilizing it. The KM ID is assumed to be known to the parties that derived the keying material. If the KM ID is not used it is set to 0. Further specification of the content of this field is outside the scope of this document.

Lifetime

The Lifetime field is an integer [RFC2865] representing the period of time (in seconds) for which the keying material is valid.

Note: Applications using this value SHOULD consider the beginning of the lifetime to be the point in time when the keying material is first used.

IV

The length of the IV field depends upon the value of the Enc Type field, but is fixed for any given value thereof. When the value of the Enc Type field is 0 (decimal), the IV field MUST be 8 octets in length (as illustrated above) and the value of the IV field MUST be as specified in [RFC3394].
Data

The Data field is variable length and contains the actual encrypted keying material.

3.2. MAC-Randomizer

Description

The MAC-Randomizer Attribute MUST be present in any message that includes an instance of the Message-Authentication-Code Attribute. The Random field MUST contain a 32 octet random number which SHOULD satisfy the requirements of [RFC4086].

Implementation Note

The Random field MUST be filled in before the MAC is computed. The MAC-Randomizer Attribute SHOULD be placed at the beginning of the RADIUS message if possible.

A summary of the MAC-Randomizer attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type (26)   |    Length   |   Vendor ID
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Vendor ID (cont’d) | Sub-type (1)| Sub-length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     String ID  ("radius:random-nonce=")
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
String ID (cont’d)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
String ID (cont’d)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
String ID (cont’d)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
String ID (cont’d)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Random...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
Type

26 for vendor specific

Length

Length of entire attribute including type and length field

Vendor ID

4 octets encoding the Cisco Vendor ID of 9

Sub-type

Attribute sub-type of 1

Sub-length

Length of the sub attribute including the sub-type and sub-length fields

String-ID

The ASCII characters "radius:random-nonce=“ without quotes or null termination.

Random

This field MUST contain a 32 octet random number which SHOULD satisfy the requirements of [RFC4086].

3.3. Message-Authentication-Code

Description

This Attribute MAY be used to "sign" messages to prevent spoofing. If it is present in a request, the receiver should take this a hint that the sender prefers the use of this Attribute for message authentication; the receiver is not obligated to do so, however.

The Message-Authentication-Code Attribute MUST be included in any message that contains a Keying-Material attribute.

Any packet that contains an instance of the Message-Authentication-Code Attribute SHOULD NOT contain an instance of the Message-Authenticator Attribute [RFC3579]. If both attributes are to be included in a message (e.g., for backward compatibility in a network containing both old and new clients), the value of
the Message-Authentication-Code Attribute MUST be computed first.

If any message is received containing an instance of the Message-Authentication-Code Attribute, the receiver MUST calculate the correct value of the Message-Authentication-Code and silently discard the packet if the computed value does not match the value received.

If a received message contains an instance of the MAC-Randomizer Attribute (Section 3.2), the received MAC-Randomizer Attribute SHOULD be included in the computation of the Message-Authentication-Code Attribute sent in the response, as described below.

A summary of the Message-Authentication-Code attribute format is shown below. The fields are transmitted from left to right.
### Type

26 for vendor specific

### Length

Length of entire attribute including type and length field
Vendor ID

4 octets encoding the Cisco Vendor ID of 9

Sub-type

Attribute sub-type of 1

Sub-length

Length of the sub attribute including the sub-type and sub-length fields

String-ID

The ASCII characters "radius:message-authenticator-code=" without quotes or null termination.

MAC Type

The MAC Type field specifies the algorithm used to create the value in the MAC field. This document defines six values for the MAC Type field:

0 HMAC-SHA-1 [FIPS.180-2.2002] [RFC2104]
1 HMAC-SHA-256 [FIPS.180-2.2002] [RFC4231]
2 HMAC-SHA-512 [FIPS.180-2.2002] [RFC4231]
3 CMAC-AES-128 [NIST.SP800-38B]
4 CMAC-AES-192 [NIST.SP800-38B]
5 CMAC-AES-256 [NIST.SP800-38B]

Implementations MUST support MAC Type 0 (HMAC-SHA-1).

MAC Key ID

The MAC Key ID field is 16 octets in length and contains an identifier for the key. The MAC Key ID MUST refer to a key of a type and length appropriate for use with the algorithm specified by the MAC Type field (see above). Further specification of the content of this field is outside the scope of this document.
MAC

Both the length and value of the MAC field depend upon the algorithm specified by the value of the MAC Type field. If the algorithm specified is HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-512, the MAC field MUST be 20, 32 or 64 octets in length, respectively. If the algorithm specified is CMAC-AES-128, CMAC-AES-192 or CMAC-AES-256, the MAC field SHOULD be 64 octets in length. The derivation of the MAC field value for all the algorithms specified in this document is identical, except for the algorithm used. There are differences, however, depending upon whether the MAC is being computed for a request message or a response. These differences are detailed below, with the free variable HASH-ALG representing the actual algorithm used.

Request Messages

For requests (e.g., CoA-Request [RFC5176], Accounting-Request [RFC2866], etc.), the value of the MAC field is a hash of the entire packet except the Request Authenticator in the header of the RADIUS packet, using a shared secret as the key, as follows.

MAC = MAC-ALG(Key, Type + Identifier + Length + Attributes)

where '+' represents concatenation

The MAC-Randomizer Attribute (Section 3.2) MUST be included in any request in which the Message-Authentication-Code Attribute is used. The Random field of the MAC-Randomizer Attribute MUST be filled in before the value of the MAC field is computed.

If the Message-Authenticator-Code Attribute is included in a client request, the server SHOULD ignore the contents of the Request Authenticator.

Implementation Notes

When the hash is calculated, both the MAC field of the Message-Authenticator-Code attribute and the String field of the Message-Authenticator Attribute (if any) MUST be considered to be zero-filled.

Implementations SHOULD provide a means to provision a key (cryptographically separate from the normal RADIUS shared secret) to be used exclusively in the generation of the Message-Authentication-Code.
Response Messages

For responses (e.g., CoA-ACK [RFC5176], Accounting-Response
[RFC2866], etc.), the value of the MAC field is a hash of
the entire packet except the Response Authenticator in the
header of the RADIUS packet using a shared secret as the
key, as follows.

\[ \text{MAC} = \text{HASH-ALG(Key, Type + Identifier + Length + Attributes)} \]

where ‘+’ represents concatenation

If the request contained an instance of the MAC-Randomizer
Attribute and the responder wishes to include an instance of
the Message-Authentication-Code Attribute in the
corresponding response, then the MAC-Randomizer Attribute
from the request MUST be included in the response.

If the Message-Authenticator-Code Attribute is included in a
server response, the client SHOULD ignore the contents of
the Response Authenticator.

Implementation Notes

When the hash is calculated, both the MAC field of the
Message-Authenticator-Code attribute and the String field
of the Message-Authenticator Attribute (if any) MUST be
considered to be zero-filled.

The Message-Authentication-Code Attribute MUST be created
and inserted in the packet before the Response
Authenticator is calculated.

Implementations SHOULD provide a means to provision a key
(cryptographically separate from the normal RADIUS shared
secret) to be used exclusively in the generation of the
Message-Authentication-Code.

4. IANA Considerations

This document does not define any actions for IANA.

5. Security Considerations

It is RECOMMENDED in this memo that two new keys, a key encrypting
key and a message authentication key, be shared by the RADIUS client
and server. If implemented, these two keys MUST be different from
each other and SHOULD NOT be based on a password. These two keys
SHOULD be cryptographically independent of the RADIUS shared secret
used in calculating the Response Authenticator [RFC2865], Request
Authenticator [RFC2866] [RFC5176] and Message-Authenticator Attribute
[RFC3579]; otherwise if the shared secret is broken, all is lost.

To avoid the possibility of collisions, the same MAC key SHOULD NOT
be used with more than $2^{(n/2)}$ messages, where ‘n’ is the length of
the MAC value in octets.

If a packet that contains an instance of the Keying-Material
Attribute also contains an instance of another, weaker key transport
attribute (e.g., MS-MPPE-Recv-Key [RFC2548]) encapsulating identical
keying material, then breaking the weaker attribute might facilitate
a known-plaintext attack against the KEK.

6. Contributors

Hao Zhou, Nancy Cam-Winget, Alex Lam, Paul Funk and John Fossaceca
all contributed to this document.

7. Acknowledgements

Thanks (in no particular order) to Keith McCloghrie, Kaushik Narayan,
Murtaza Chiba, Bill Burr, Russ Housley, David McGrew, Pat Calhoun,
Joel Halpern, Jim Schaad and Greg Weber for useful feedback.

8. References

8.1. Normative References

[FIPS.180-2.2002]
National Institute of Standards and Technology, "Secure

[NIST.SP800-38B]
Dworkin, M., "Recommendation for Block Cipher Modes of

[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
Informative References


Authors’ Addresses

Glen Zorn
Network Zen
1463 East Republican Street
#358
Seattle, WA  98112
US
Email: gwz@net-zen.net

Tiebing Zhang
Advista Technologies
5252 Orange Ave, Suite 108
Cypress, CA  90630
US
Phone: +1 (949) 242 0391
Email: tzhang@advistatech.com

Jesse Walker
Intel Corporation
JF3-206
2111 N.E. 25th Ave
Hillsboro, OR  97214-5961
US
Phone: +1 (503) 712-1849
Email: jesse.walker@intel.com

Joseph Salowey
Cisco Systems
2901 Third Avenue
SEA1/6/
Seattle, WA  98121
US
Phone: +1 (206) 256-3380
Email: jsalowey@cisco.com