RADIUS Extensions for IEEE 802

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on January 2, 2005.

Copyright Notice

Copyright (C) The Internet Society 2004. All rights reserved.

Abstract

IEEE 802.1X-2004 enables authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless LANs. Although AAA support is optional within IEEE 802.1X, it is expected that many IEEE 802.1X Authenticators will function as RADIUS or Diameter clients (or both).

This document proposes additional attributes for usage by IEEE 802.1X authenticators. These attributes are usable within either RADIUS or Diameter.
Table of Contents

1. Introduction ............................................. 3
   1.1 Terminology .................................... 3
   1.2 Requirements Language .......................... 4
   1.3 Attribute format ................................ 4

2. RADIUS Authentication ..................................... 5
   2.1 Egress-VLANID ................................... 5
   2.2 Ingress-Filters .................................. 6
   2.3 User-Priority-Table ............................. 7
   2.4 Allowed-SSID ..................................... 8
   2.5 Allowed-Called-Station-Id ....................... 9
   2.6 NAS-Filter-Rule .................................. 9
   2.7 QoS-Filter-Rule .................................. 10
   2.8 EAP-Master-Session-Key .......................... 11
   2.9 EAP-Key-Name .................................... 12
   2.10 Redirect-Host ................................... 12
   2.11 Origin-Realm ..................................... 13

3. RADIUS Accounting .......................................... 14
   3.1 Accounting-EAP-Auth-Method ....................... 14

4. Table of Attributes ......................................... 14

5. Diameter Considerations .................................... 15

6. IANA Considerations ........................................ 17

7. Security Considerations .................................... 17
   7.1 Packet modification or forgery .................. 17
   7.2 Dictionary Attacks .................................. 18
   7.3 Known Plaintext Attacks .......................... 18
   7.4 Key Management Issues ............................ 19

8. References ................................................ 19
   8.1 Normative References ............................... 19
   8.2 Informative References ............................. 21

Appendix A - Extended Attribute Formats ..................... 23

Acknowledgements ........................................... 27
Authors’ Addresses .......................................... 27
Intellectual Property Statement ............................ 27
Disclaimer of Validity ..................................... 28
Full Copyright Statement ................................... 28
1. Introduction

IEEE 802.1X [IEEE8021X] provides "network port authentication" for IEEE 802 [IEEE802] media, including Ethernet [IEEE8023], Token Ring and 802.11 [IEEE80211] wireless LANS.

IEEE 802.1X does not require use of a backend authentication server, and thus can be deployed with stand-alone bridges or Access Points, as well as in centrally managed scenarios. As a result, support for the RADIUS [RFC2865] or Diameter [RFC3588] protocols is optional for IEEE 802.1X authenticators.

In situations where it is desirable to centrally manage authentication, authorization and accounting (AAA) for IEEE 802 networks, deployment of a backend authentication and accounting server is desirable. In such situations, it is expected that IEEE 802.1X authenticators will function as AAA clients. This document defines additional attributes suitable for usage by IEEE 802.1X authenticators acting as AAA clients.

1.1. Terminology

This document uses the following terms:

Access Point (AP)
A Station that provides access to the distribution services via the wireless medium for associated Stations.

Association
The service used to establish Access Point/Station mapping and enable Station invocation of the distribution system services.

Authenticator
An authenticator is an entity that require authentication from the supplicant. The authenticator may be connected to the supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.

Authentication server
An authentication server is an entity that provides an authentication service to an authenticator. This service verifies from the credentials provided by the supplicant, the claim of identity made by the supplicant.

Port Access Entity (PAE)
The protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the protocol functionality associated with the Authenticator, Supplicant or...
both.

Station (STA)
Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

Supplicant
A supplicant is an entity that is being authenticated by an authenticator. The supplicant may be connected to the authenticator at one end of a point-to-point LAN segment or 802.11 wireless link.

1.2. Requirements Language

In this document, several words are used to signify the requirements of the specification. 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].

1.3. Attribute format

In defining the attributes included in this document, a number of problems were encountered, including issues with RADIUS/Diameter translation and negotiation of support for security-critical attributes.

Since support for RADIUS or Diameter protocols is optional for IEEE 802.1X authenticators, it is desirable for attributes defined for use with [IEEE8021X] to be usable within both RADIUS and Diameter, ideally without the need to define elaborate gateway translation rules as in [NASREQ]. This issue was not encountered in [RFC3580] since that document did not define any new attributes, while this specification does.

Several of the attributes proposed in this document have security implications. If sent by a RADIUS server to a RADIUS client, these attributes may not be safely ignored, or the required security will not be provided. As noted in [RFC2865] Section 5:

- A RADIUS server MAY ignore Attributes with an unknown Type.
- A RADIUS client MAY ignore Attributes with an unknown Type.

Unfortunately, in the case of security-critical attributes, the behavior that is desired is for the RADIUS client to deny access to the network on receipt of unknown attributes, rather than ignoring them.
In order to enable the RADIUS client to distinguish unknown attributes that may be safely ignored from attributes that must be understood in order to safely provide service, security-critical attributes need to be encoded using an attribute format which includes support for a Mandatory bit. The use of the Mandatory bit needs to be negotiated so that it will only be assumed to be usable by the RADIUS server if the RADIUS client indicates support for it.

Several possible mechanisms suggest themselves for dealing with RADIUS/Diameter translation problems and the need for a Mandatory bit. For example, it is possible for IEEE 802 to define a Vendor-Specific Attribute (VSA) format that can accommodate a Mandatory bit. Another alternative is to utilize an Extended RADIUS attribute format, as proposed by [Arkko]. Other solutions are possible as well. However, for the purpose of this document, it is not necessary to take a position on the preferred approach, only to point out that we believe that these problems need to be solved.

For the purposes of illustrating some potential alternatives, Appendix A describes a potential Extended attribute format based on [Arkko], and suggests how usage might be negotiated between the RADIUS client and server. Potential modifications to enable support for sub-attributes and a more efficient "short form" encoding are also described. For the purposes of calculating the attribute Length field of extended attributes, the "short form" encoding described in Appendix A is assumed.

2. RADIUS Authentication

2.1. Egress-VLANID

Description

The Egress-VLANID attribute represents an allowed IEEE 802 Egress VLANID for this port. The Egress-VLANID contains two parts: the first part is the VLANID, the second part indicates if this VLANID is allowed for tagged or untagged packets.

Multiple Egress-VLANID attributes can be delivered in an authentication response; each attribute adds the specified VLAN to the list of allowed egress VLANs for the port. This is an Extended RADIUS attribute.

Code

TBD

Length
2.2. Ingress-Filters

Description

802.1Q clause 8.4.5 describes the Ingress Filter variable per port. The Ingress-Filters attribute corresponds to Ingress Filter per-port variable defined in IEEE 802.1Q clause 8.4.5. When the attribute has the value "Enabled", the set of VLANs that are allowed to ingress a port must match the set of VLANs that are allowed to egress a port. By default, where the Ingress-Filter attribute is not set, the value "Disabled" should be assumed. Only a single Ingress-Filters attribute MAY be sent within an Access-Accept or CoA-Request; this attribute MUST NOT be sent within an Access-Request, Access-Challenge, Access-Reject, or Disconnect-Request.

This attribute is defined as an Extended RADIUS attribute.

Code

TBD

Length

8

M

1 - Mandatory

Data-Type

Integer32

The values include:

1 = Tagged
2 = Untagged
2.3. User-Priority-Table

Description

IEEE 802.1D clause 7.5.1 discusses how to regenerate (or re-map) user priority on frames received at a port. This per-port configuration enables a bridge to cause the priority or received traffic at a port to be mapped to a particular priority. The management variables are described in clause 14.6.2.2.

This attribute represents the IEEE 802 prioritization that will be applied to packets arriving at this port. There are eight possible user priorities, according to the IEEE 802 standard.

This attribute is defined as an Extended RADIUS attribute.

Code

TBD

Length

12

M

1 - Mandatory

Data-Type

UInt64

The table, expressed as a unsigned 64-bit integer, maps the incoming priority (if one exists - the default is 0) into one of seven regenerated priorities. The format of this attribute is an eight byte octet string, where the first octet maps to incoming priority 0, the second octet to incoming priority 1, etc. The values in each octet represent the regenerated priority of the packet.
It is thus possible to either remap incoming priorities to more appropriate values; or to honor the incoming priorities; or to override any incoming priorities, forcing them to all map to a single chosen priority.

The IEEE 802.1D specification, Annex G, provides a useful description of traffic type - traffic class mappings.

For mapping of the priority to quality of service at the IP layer, it is assumed that the LAN Edge Device has been provided a table with device-wide mappings of this user priority to the appropriate DiffServ code points. That table and its configuration are outside the scope of this document.

2.4. Allowed-SSID

Description

As described in [KEYFRAME] Section 2.5, it may be desirable for the RADIUS server to be able to restrict the scope of the EAP Key provided to the RADIUS client. In particular, it may be desirable to restrict the use of the key to a set of authorized SSIDs.

The Allowed-SSID attribute allows the RADIUS server to specify which SSIDs the user is allowed to access. More than one Allowed-SSID attribute may be included in an Access-Accept packet. This attribute is defined as an Extended RADIUS attribute. The Allowed-SSID attribute is defined as follows:

Code

TBD

Length

>=5

M

1 - Mandatory

Data-Type

String

String

The String field contains one or more octets, encoding a single
SSID, as defined in [IEEE80211]. UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

2.5. Allowed-Called-Station-Id

Description

As described in [KEYFRAME] Section 2.5, it may be desirable for the RADIUS server to be able to restrict the scope of the AAA-Key provided to the RADIUS client. In particular, it may be desirable to restrict the use of the key to a set of authorized Called-Station-Ids. The Allowed-Called-Station-Id attribute allows the RADIUS server to specify which Called-Station-Ids the user is allowed to access. More than one Allowed-Called-Station-Id attribute may be included in an Access-Accept packet. This attribute is defined as an Extended RADIUS attribute. The Allowed-Called-Station-Id attribute is defined as follows:

Code

TBD

Length

>=5

M

1 - Mandatory

Data-Type

String

String

The String field is one or more octets, containing the layer 2 endpoint that the user’s call terminated on. For details of the encoding, see [RFC3580]. UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

2.6. NAS-Filter-Rule

Description

The NAS-Filter-Rule attribute enables the provisioning of Internet
Protocol filters on the NAS by the RADIUS server. This attribute is defined as an Extended RADIUS attribute. The NAS-Filter-Rule attribute is defined as follows:

Code

400 [NASREQ]

Length

>=5

M

1 - Mandatory

Data-Type

IPFilterRule

The IPFilterRule field contains an IP filter, utilizing the syntax defined for the IPFilterRule derived data type defined in [RFC3588], Section 4.3. Since the NAS-Filter-Rule AVP defined in [NASREQ] Section 6.6 also obeys the same syntax, these attributes are analogous.

2.7. QoS-Filter-Rule

Description

The QoS-Filter-Rule attribute enables the provisioning of QoS filters on the NAS by the RADIUS server. This attribute is defined as an Extended RADIUS attribute. The QoS-Filter-Rule attribute is defined as follows:

Code

407

Length

>=5

M

1 - Mandatory
Data-Type

QoSFilterRule

QoSFilterRule

The QoSFilterRule field contains a QoS filter, utilizing the syntax defined for the QoSFilterRule derived data type defined in [RFC3588], Section 4.3. Note that this definition contained an error, so that the complete syntax is described in the definition of the QoS-Filter-Rule AVP, defined in [NASREQ] Section 2.

2.8. EAP-Master-Session-Key

Description

The EAP-Master-Session-Key attribute enables a RADIUS server to provide an EAP Master Session Key to the RADIUS client, as defined in [KEYFRAME]. This attribute MUST NOT be included in an Access-Request or Access-Challenge, but MAY be included within an Access-Accept. This attribute is defined as an Extended RADIUS attribute. The EAP-Master-Session-Key attribute is defined as follows:

Code

TBD [DiamEAP]

Length

>=12

M

1 - Mandatory

Data-Type

String

String

The String field is eight or more octets, containing the EAP Master Session Key provided to the RADIUS client. In order to address the RADIUS security threats detailed in [RFC3579] Section 4.3, IPsec ESP with non-null transform MUST be used to protect RADIUS packets containing this attribute, as described in [RFC3579], Section 4.2. As a result, there is no need for alternative confidentiality mechanisms.
2.9. EAP-Key-Name

Description

The EAP-Key-Name attribute enables a RADIUS server to provide a key name to the RADIUS client. It should be noted that not all link layers use this attribute, and currently most EAP methods do not generate it. If sent within an Access-Request, the EAP-Key-Name attribute MUST be empty (Length = 4), and a RADIUS server SHOULD include this attribute in an Access-Accept only if an empty EAP-Key-Name attribute was present in the Access-Request. This attribute MUST NOT be included within an Access-Challenge. This attribute is defined as an Extended RADIUS attribute. The EAP-Key-Name attribute is defined as follows:

Code

TBD [DiamEAP]

Length

= 4 (REQUIRED in an Access-Request)

>=5 (REQUIRED in an Access-Accept)

M

1 - Mandatory

Data Type

String

String

The String field is one or more octets, containing the name of the key provided to the RADIUS client. For details of the encoding, see [KEYFRAME], and [DiamEAP], Section 4.1.4. UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

2.10. Redirect-Host

Description

The Redirect-Host attribute provides support for Redirect functionality, as described in [RFC3588], Section 6.12. This attribute is defined as an Extended RADIUS attribute.
Code

? - Defined in [RFC3588]

Length

=4 (REQUIRED in an Access-Request)
>=5 (REQUIRED in an Access-Accept)

M

1 - Mandatory

Data Type

String

String

The String field is one or more octets, containing the full qualified domain name of the server to which the NAS should be redirected. This attribute MUST only be sent in an Access-Accept if a null Redirect-Host attribute (Length = 4) is included in an Access-Request.

2.11. Origin-Realm

Description

The Origin-Realm attribute contains the realm of the originator of a message, as described in [RFC3588], Section 6.4.

Code

296

Length

>=5 (Short Form)

M

1 - Mandatory

Data Type

String

String
The String field contains the fully qualified domain name (FQDN) representing the realm.

3. RADIUS Accounting

3.1. Accounting-EAP-Auth-Method

Description

Accounting-EAP-Auth-Method enables a RADIUS client to include the EAP method utilized within an accounting packet. The semantics of this attribute are identical to that of the Accounting-EAP-Auth-Method AVP defined in [DiamEAP], Section 4.1.5. This is a standard RADIUS attribute.

The Accounting-EAP-Auth-Method attribute 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      |    Length     |            Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBD

Length

10

Value

The Value field is eight octets. In case of expanded types defined in [RFC3748] Section 5.7, the least significant 32 bits contain the Vendor-Type field, and the next 24 bits contain the Vendor-Id field.

4. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.
<table>
<thead>
<tr>
<th>Access-Request</th>
<th>Access-Accept</th>
<th>Access-Reject</th>
<th>Access-Challenge</th>
<th>CoA-Req</th>
<th>#</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>TBD</td>
<td>Extended</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0+</td>
<td>TBD</td>
<td>Egress-VLANID [a]</td>
</tr>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>0-1</td>
<td>TBD</td>
<td>Ingress-Filters [a]</td>
</tr>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>0-1</td>
<td>TBD</td>
<td>User-Priority-Table [a]</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>Allowed-SSID</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>Allowed-Called-Station-Id</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0+</td>
<td>TBD</td>
<td>NAS-Filter-Rule [a]</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0+</td>
<td>TBD</td>
<td>QoS-Filter-Rule [a]</td>
</tr>
<tr>
<td>0-1</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>EAP-Master-Session-Key</td>
</tr>
<tr>
<td>0-1</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>EAP-Key-Name</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>Redirect-Host</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>296</td>
<td>Origin-Realm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actng-Request</th>
<th>Actng-Response</th>
<th>#</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>0</td>
<td>TBD</td>
<td>Accounting-EAP-Auth-Method</td>
</tr>
</tbody>
</table>

The following table defines the meaning of the above table entries.

<table>
<thead>
<tr>
<th></th>
<th>This attribute MUST NOT be present in packet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Zero or more instances of this attribute MAY be present in the packet.</td>
</tr>
<tr>
<td>0-1</td>
<td>Zero or one instance of this attribute MAY be present in the packet.</td>
</tr>
</tbody>
</table>

Notes
-----
[a] This attribute MAY only be included in a CoA-Request if the NAS indicates in the Access-Request that it supports Extended attributes. Otherwise, this attribute MUST NOT be sent in a CoA-Request.

5. Diameter Considerations

As described in Appendix A, the Extended attributes described in this specification are defined in both RADIUS and Diameter, and utilize the Data Types defined in [RFC3588]. Attributes already defined within Diameter, and defined as Extended RADIUS attributes within this specification include: NAS-Filter-Rule [NASREQ], QoS-Filter-Rule [NASREQ], EAP-Master-Session-Key [DiamEAP], EAP-Key-Name [DiamEAP], Redirect-Host [RFC3588] and Origin-Realm [RFC3588].

Extended attributes defined within both RADIUS and Diameter include Egress-VLANID, Ingress-Filters, User-Priority-Table, Allowed-SSID, and Allowed-Called-Station-Id.

Attributes solely defined within RADIUS include the Extended
attribute (used to encapsulate Diameter-compatible RADIUS attributes), as well as the Accounting-EAP-Auth-Method attribute, defined within [DiamEAP].

In order to translate RADIUS Extended attributes to Diameter AVPs, a RADIUS/Diameter gateway must first concatenate all RADIUS attributes of type Extended, and then parse the included sub-attributes. The sub-attributes are then encapsulated within the Diameter AVP format as follows:

a. The Code, Length, and Mandatory fields as well as the attribute data are copied directly from the Extended RADIUS attribute to the Diameter AVP.

b. If the RADIUS "short form" Extended format is used, then the 'V' bit always set to zero in the Diameter AVP.

c. If the RADIUS "long form" Extended format is used, then the 'V' bit and Vendor-Id is copies from the Extended RADIUS attribute to the Diameter AVP.

In translating from Diameter to RADIUS, the gateway encapsulates Diameter AVPs within Extended RADIUS attributes as follows:

a. If the 'V' bit is set to one (1), or the Diameter AVP Code is larger than 16384, then the "Long Form" Extended RADIUS attribute format MUST be used. Otherwise, the "Short Form" attribute format SHOULD be used.

b. The Code, Length, and Mandatory fields as well as the attribute data are copied directly from the Diameter AVP to the Extended RADIUS attribute.

c. If the 'V' bit is set to one (1), then the 'V' bit as well as the Vendor-Id fields are copies from the Diameter AVP to the Extended RADIUS attribute.

d. Once the Extended RADIUS attributes have been encoded, they are encapsulated within RADIUS attributes of type Extended.

Note that automated translation may not be on an initial Access-Request, since this packet must contain an empty Extended attribute in order to negotiate use of the Extended attribute format.
6. IANA Considerations

This specification does not create any new registries.

This specification requires assignment of a RADIUS attribute type for the Extended attribute. In addition, this specification requires assignment of the following Diameter Code values:

<table>
<thead>
<tr>
<th>AVP</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress-VLANID</td>
<td>TBD</td>
</tr>
<tr>
<td>Ingress-Filter-Enable</td>
<td>TBD</td>
</tr>
<tr>
<td>User-Priority-Table</td>
<td>TBD</td>
</tr>
<tr>
<td>Allowed-SSID</td>
<td>TBD</td>
</tr>
<tr>
<td>Allowed-Called-Station-Id</td>
<td>TBD</td>
</tr>
</tbody>
</table>
7.2. Dictionary Attacks

As discussed in [RFC3579] Section 4.3.3, the RADIUS shared secret is vulnerable to offline dictionary attack, based on capture of the Response Authenticator or Message-Authenticator attribute. In order to decrease the level of vulnerability, [RFC2865], Section 3 recommends:

The secret (password shared between the client and the RADIUS server) SHOULD be at least as large and unguessable as a well-chosen password. It is preferred that the secret be at least 16 octets.

In addition, the risk of an offline dictionary attack can be further mitigated by employing IPsec ESP with non-null transform in order to encrypt the RADIUS conversation, as described in [RFC3579], Section 4.2.

7.3. Known Plaintext Attacks

Since IEEE 802.1X is based on EAP, which does not support PAP, the RADIUS User-Password attribute is not used to carry hidden user passwords. The hiding mechanism utilizes MD5, defined in [RFC1321], in order to generate a key stream based on the RADIUS shared secret and the Request Authenticator. Where PAP is in use, it is possible to collect key streams corresponding to a given Request Authenticator value, by capturing RADIUS conversations corresponding to a PAP authentication attempt using a known password. Since the User-Password is known, the key stream corresponding to a given Request Authenticator can be determined and stored.

The vulnerability is described in detail in [RFC3579], Section 4.3.4. Even though IEEE 802.1X Authenticators do not support PAP authentication, a security vulnerability can still exist where the same RADIUS shared secret is used for hiding User-Password as well as other attributes. This can occur, for example, if the same RADIUS proxy handles authentication requests for both IEEE 802.1X (which may hide the Tunnel-Password, MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes) and GPRS (which may hide the User-Password attribute).

The threat can be mitigated by protecting RADIUS with IPsec ESP with non-null transform, as described in [RFC3579], Section 4.2. In addition, the same RADIUS shared secret MUST NOT used for both IEEE 802.1X authentication and PAP authentication.
7.4. Key Management Issues

As detailed in [Housley56], AAA protocols transporting keys are required to protect them against disclosure to third parties. After much debate, the AAA WG has settled on the Diameter re-direct mechanism to enable transport of keys directly between the NAS and the home AAA server.

The redirect key protection mechanism relies on scalable mechanisms for establishment of security associations between the NAS and home AAA server, such as provisioning of certificates. This can be accommodated by use of RADIUS over IPsec, as specified in [RFC3579].

As described in Section 2.10, support for the redirect key protection mechanism also requires addition of a Redirect attribute to RADIUS. As in [DiamEAP], the NAS can either attempt to use a re-direct to directly communicate with the home server from the beginning, or it can request authentication-only while communicating through proxies, and then can send an authorize-only message directly to the home-server to obtain the key.

Note that this usage may not work well with existing RADIUS implementations that interpret key attributes as authentication, rather than authorization-related.

8. References

8.1. Normative references


8.2. Informative references


[IEEE80211] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std 802.11-1999

[KEYFRAME]

Appendix A - Extended Attribute Formats

The use of a Diameter-compatible Extended attribute format within RADIUS was first proposed in [Arkko]. This Appendix describes a potential definition of the Extended attribute, based on a modified version of that proposal. The proposed definition provides support for Diameter-compatibility as well as sub-attributes, and support for a more efficient "short form" encoding.

The Extended attribute, RADIUS attribute type TBD, enables the encoding of Extended RADIUS attributes. If multiple Extended attributes are present in a packet their values should be concatenated; this allows attributes longer than 253 octets to be transported by the Extended attribute format. Multiple sub-attributes MAY be encoded within a single Extended attribute, although they do not have to be.

Note: for the purposes of this appendix, allocation of a new RADIUS Type value is assumed. However, on the RADEXT WG mailing list, there has also been discussion of utilizing type 26 (Vendor-Specific) along with a Vendor-Id of zero(0). For the purposes of this specification either format would be work equally well.

Extended attributes MUST only be used when both the RADIUS client and server support them. A RADIUS client supporting the Extended attribute format MUST include an Extended attribute with a Length value of two (2) within the initial Access-Request of a session. A RADIUS server receiving an empty Extended attribute within an Access-Request MAY utilize Extended attributes within messages sent to the client, including Access-Reject, Access-Challenge, Access-Accept, CoA-Request and Disconnect-Request messages.

A RADIUS server not receiving an empty Extended attribute within an initial Access-Request MUST NOT include Extended attributes in any RADIUS message sent to the client, including Access-Reject, Access-Challenge, Access-Accept, CoA-Request or Disconnect-Request messages.
A.1 - Full Diameter AVP Format

The full Extended attribute format is defined as follows:

```
+--------+--------+--------+--------+
|        |        |        |        |
| 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   | Length | S      | Code   |
+--------+--------+--------+--------+
|        |        |        |        |
| Code (opt) | Length2 |
+--------+--------+--------+
|        |        |        |        |
| Flags  | Vendor-Id (opt) |
+--------+--------+
|        |        |        |        |
| Vendor-Id (opt) | Data... |
+--------+
```

Type

TBD - Allocated by IANA from within the RADIUS attribute space.

Length

The length of the attribute in octets, including the Type, Length, S, Code, Length2, Flags, Vendor-Id and Data fields.

S

0 - Full Diameter AVP format
1 - Short Form

Code

Where the S bit is clear, the "full Diameter AVP" format is used, and the Code field is 31 bits, encoding the 31 least significant bits of the Diameter AVP format defined in [RFC3588].

Where the S bit is set, the "Short Form" Extended format is used, and the Code field is 14 bits, encoding the 14 least significant bits of the Diameter AVP format, defined in [RFC3588].

Length2

The Length of the sub-attribute in octets, including the S, M, Code, Length2 and Data fields.

Flags

The Flags field is a single octet, defined as follows:
V

0 = IETF standard
1 = Vendor Specific

M

The ‘M’ Bit, known as the Mandatory bit, indicates whether support of the attribute is required. If an attribute with the ‘M’ bit set is received and either the attribute or its value is unrecognized, the message MUST be silently discarded.

Attributes with the ‘M’ bit cleared are informational only and a receiver that receives a message with such an attribute that is not supported, or whose value is not supported, MAY simply ignore the attribute.

r

The ‘r’ (reserved) bits are unused and SHOULD be set to 0. Note that subsequent specifications MAY define additional bits within the header, and an unrecognized bit SHOULD be considered an error.

Vendor-Id

The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order.

Data

The Data field is zero or more octets and contains information specific to the attribute. The format and length of the Data field is determined by the Code and Length2 fields. The format of the Data field MUST be one of the data types defined in [RFC3588] or a data type derived from the base data types.

A.2 - Short Form

In order to enable Extended attributes to be encoded more economically, a "Short Form" of the Extended attribute format is proposed. The Short Form can be used to encode any Diameter AVP that meets the following constraints:
[a] An IETF standard attribute (not Vendor-Specific)
[b] Diameter Code between 0 and 16384 (all existing attributes)
[c] No flag bits other than the Mandatory bit.

The short form Extended attribute format is defined as follows:

```
|     Type      |  Length       |S|M|            Code           |
|---------------|---------------|---|--------------------------|
|               |               |   |                          |
```

Where:
- **Type**: TBD - Allocated by IANA from the RADIUS attribute space.
- **Length**: The length of the attribute in octets, including the Type, Length, S, M, Code, Length2 and Data fields.
- **S**: 1 - Short Form
- **M**: 0 - Optional
  1 - Mandatory
- **Code**: The 14 least significant bits of the Diameter AVP Code field, as defined in [RFC3588].
- **Length2**: The Length of the sub-attribute in octets, including the S, M, Code, Length2 and Data fields.
- **Data**: The Data field is zero or more octets and contains information specific to the attribute. The format and length of the Data field is determined by the Code and Length2 fields. The format of the Data field MUST be one of the data types defined in {Congdon, et al. Informational [Page 26]}

{Congdon, et al. Informational [Page 26]}

{Congdon, et al. Informational [Page 26]}
Acknowledgments

The authors would like to acknowledge Dorothy Stanley of Agere, and Ashwin Palekar of Microsoft.

Authors' Addresses

Paul Congdon
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662
Roseville, CA  95747
EMail: paul.congdon@hp.com
Phone: +1 916 785 5753
Fax:   +1 916 785 8478

Chuck Black
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662
Roseville, CA  95747
EMail: chuck.black@hp.com
Phone: +1 916 785 9713
Fax:   +1 916 785 1199

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA  98052
EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax:   +1 425 936 7329

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation
can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.