Network Working Group   Bernard Aboba
INTERNET-DRAFT   Microsoft
Category: Proposed Standard
<draft-aboba-radext-wlan-00.txt>
3 July 2005

RADIUS Attributes for WLAN

Abstract

IEEE 802.11i defines the use of EAP authentication with IEEE 802.11 wireless LANs. Although AAA support is optional within IEEE 802.11i, it is expected that many IEEE 802.11i authenticators will function as AAA clients. This document proposes additional attributes for use by IEEE 802.11 authenticators. The attributes defined in this document are compatible with those used within Diameter EAP.

Table of Contents

1. Introduction

In situations where it is desirable to centrally manage authentication, authorization and accounting (AAA) for IEEE 802.11 wireless LANs, deployment of a backend authentication and accounting server is desirable. In such situations, it is expected that IEEE 802.11 authenticators will function as AAA clients. This document defines additional attributes suitable for usage by IEEE 802.11 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.

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].

2. RADIUS Attributes

2.1. 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 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 SSIDs. The Allowed-SSID attribute allows the RADIUS server to specify which SSIDs the user is allowed to access. One or more Allowed-SSID attributes MAY be included an Access-Accept packet. This attribute is not allowed in other RADIUS packets. A summary of the Allowed-SSID 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD

Length

>=3

String

The String field contains one or more octets, encoding a single SSID, as defined in [IEEE-802.11]. UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

2.2. 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 not allowed in other RADIUS packets. A summary of the Allowed-Called-Station-ID 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD

Length

>=3

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 [RFC2865] and [RFC3580]. A robust implementation SHOULD support the field as undistinguished octets.

2.3. EAP-Key-Name

Description

The EAP-Key-Name Attribute contains the key name associated with the EAP-Master-Session-Key attribute. Exactly how this attribute is used depends on the link layer in question. See [KEYFRAME] for more discussion.

It should be noted that not all link layers use this name and existing EAP method implementations do not generate it. An EAP-

Key-Name attribute MAY only be included within Access-Request and Access-Accept packets. A summary of the EAP-Key-Name 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |          String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD [DiamEAP]

Length

>=3

String

The String field, when present, is one or more octets, containing the EAP Session-ID, as defined in [KEYFRAME] Section 2.4. Since the NAS operates as a pass-through in EAP, it cannot know the EAP Session-ID before receiving it from the RADIUS server. As a result, an EAP-Key-Name attribute sent in an Access-Request MUST NOT contain any data. A RADIUS server receiving an Access-Request with a EAP-Key-Name attribute with non-empty data MUST silently discard the attribute. In addition, the RADIUS server SHOULD include this attribute in an Access-Accept only if an empty EAP-Key-Name attribute was present in the Access-Request.

2.4. EAP-Master-Session-Key

Description

The EAP-Master-Session-Key Attribute contains an EAP Master Session Key (MSK), used as keying material for protecting the communications between the user and the NAS. Exactly how this keying material is used depends on the link layer in question, and is beyond the scope of this document. For more discussion on the MSK, see [RFC3748] and [KEYFRAME]. The EAP-Master-Session-Key attribute MAY be included in a RADIUS Access-Accept. This attribute is not allowed in other RADIUS packets.

```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD [DiamEAP]

Length

>=3

String

The String field is one or more octets, containing an EAP Master Session Key (MSK), encrypted using AES Key Wrap with 128-bit KEK as described in [RFC3394] Section 4.1.

The KEK is derived from the RADIUS shared secret (K) and the Request Authenticator (R) as follows:

KEK = PRF(K, "EAP MSK KEK" || R, 128)

The PRF algorithm is based on PRF+ from IKEv2 shown below ("|" denotes concatenation)

K = Key, S = Seed, LEN = output length, represented as binary in a single octet.

PRF (K,S,LEN) = T1 | T2 | T3 | T4 | ... where:

T1 = HMAC-SHA256(K, S | LEN | 0x01)
T2 = HMAC-SHA256(K, T1 | S | LEN | 0x02)
T3 = HMAC-SHA256(K, T2 | S | LEN | 0x03)
T4 = HMAC-SHA256(K, T3 | S | LEN | 0x04)

2.5. EAP-Peer-ID

Description

The EAP-Peer-ID Attribute contains an the Peer-ID generated by the EAP method. Exactly how this name is used depends on the link layer in question. See [KEYFRAME] for more discussion. The EAP-Peer-ID attribute is only allowed in Access-Request and Access-Accept packets.

It should be noted that not all link layers use this name, and existing EAP method implementations do not generate it. Since the NAS operates as a pass-through in EAP, it cannot know the EAP-Peer-ID before receiving it from the RADIUS server. As a result, an EAP-Peer-ID attribute sent in an Access-Request MUST NOT contain any data. A home RADIUS server receiving an Access-Request an EAP-Peer-ID attribute with non-empty data MUST silently discard the attribute. In addition, the home RADIUS server SHOULD include this attribute an Access-Accept only if an empty EAP-Peer-ID attribute was present in the Access-Request. An EAP-Peer-ID attribute MUST NOT be included within an Access-Challenge. A summary of the EAP-Peer-ID 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD

Length

>=3

String

The String field is one or more octets, containing the EAP Peer-ID exported by the EAP method. For details, see [KEYFRAME] Appendix E. A robust implementation SHOULD support the field as undistinguished octets.

2.6. EAP-Server-ID

Description

The EAP-Server-ID Attribute contains the Server-ID generated by the EAP method. Exactly how this name is used depends on the link layer in question. See [KEYFRAME] for more discussion. The EAP-Server-ID attribute is only allowed in Access-Request and Access-Accept packets.

It should be noted that not all link layers use this name, and existing EAP method implementations do not generate it. Since the NAS operates as a pass-through in EAP, it cannot know the EAP-

Server-ID before receiving it from the RADIUS server. As a result, an EAP-Server-ID attribute sent in an Access-Request MUST NOT contain any data. A home RADIUS server receiving in an Access-Request an EAP-Server-ID attribute with non-empty data MUST silently discard the attribute. In addition, the home RADIUS server SHOULD include this attribute an Access-Accept only if an empty EAP-Server-ID attribute was present in the Access-Request. An EAP-Server-ID attribute MUST NOT be included within an Access-Challenge. A summary of the EAP-Server-ID 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD

Length

>=3

String

The String field is one or more octets, containing the EAP Server-ID exported by the EAP method. For details, see [KEYFRAME]. A robust implementation SHOULD support the field as undistinguished octets.

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. The Accounting-EAP-Auth-Method attribute is only allowed in Accounting-Request packets.

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 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |  Length       |             Vendor-ID         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Vendor-ID            |            Vendor-Type
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Vendor-Type          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBD [DiamEAP]

Length

10

Vendor-ID

The Vendor-Id is 4 octets and represents the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as allocated by IANA. A Vendor-Id of zero is reserved for use by the IETF in providing an expanded global EAP Type space.

Vendor-Type

The Vendor-Type field is four octets and represents the vendor-specific EAP method Type. If the Vendor-Id is zero, the Vendor-Type field is an extension and superset of the existing namespace for EAP Types. For more information, see [RFC3748], Section 5.7.

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.

Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Req	#	Attribute
0	0+	0	0	0	TBD	Allowed-SSID
0	0+	0	0	0	TBD	Allowed-Called-Station-Id
0-1	0-1	0	0	0	TBD	EAP-Key-Name
0	0-1	0	0	0	TBD	EAP-Master-Session-Key
0-1	0-1	0	0	0	TBD	EAP-Peer-ID
0-1	0-1	0	0	0	TBD	EAP-Server-ID

Actng-Request	Actng-Response	#	Attribute
0-1	0	TBD	Accounting-EAP-Auth-Method

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

0	This attribute MUST NOT be present in packet.
0+	Zero or more instances of this attribute MAY be present in the packet.
0-1	Zero or one instance of this attribute MAY be present in the packet.

5. Diameter Considerations

Several of the attributes described in this document are already defined as RADIUS attributes within Diameter EAP. These include EAP-Key-Name [DiamEAP], EAP-Master-Session-Key [DiamEAP] and Accounting-EAP-Auth-Method [DiamEAP].

Since Diameter packets are always encrypted, within Diameter EAP the EAP-Master-Session-Key AVP is always sent in cleartext. However in RADIUS encryption may not be used, so that the EAP-Master-Session-Key attribute needs to be encrypted on a hop-by-hop basis, using the RADIUS shared secret.

New attributes not previously defined in Diameter EAP include EAP-Peer-ID, EAP-Server-ID, Allowed-SSID and Allowed-Called-Station-ID. When used with Diameter EAP, all of these attributes should be considered optional.

6. IANA Considerations

This specification does not create any new registries.

This specification requires assignment of a RADIUS attribute types for the following attributes:

Attribute	Type
Allowed-SSID	TBD
Allowed-Called-Station-Id	TBD
EAP-Peer-ID	TBD
EAP-Server-ID	TBD

7. Security Considerations

Since this document describes the use of RADIUS for purposes of authentication, authorization, and accounting in WLANs, it is

vulnerable to all of the threats that are present in other RADIUS applications. For a discussion of these threats, see [RFC2607], [RFC2865], [RFC3162], [RFC3576], [RFC3579], and [RFC3580].

However, there are several additional threats worth discussing:

Dictionary attacks
Key management issues

7.1. 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. The use of AES Keywrap to protect the EAP-Master-Session-Key attribute does not mitigate this vulnerability, since an attacker obtaining the RADIUS shared secret will have all the information necessary to obtain the EAP MSK.

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 reduced by employing IPsec ESP with non-null transform in order to encrypt the RADIUS conversation, as described in [RFC3579], Section 4.2.

7.2. Key Management Issues

As detailed in [Housley], AAA protocols transporting keys are required to protect them against disclosure to third parties. In Diameter EAP [DiamEAP] this is accomplished by use of the Diameter re-direct mechanism, enabling transport of keys directly between the NAS and the home AAA server.

Diameter redirect relies on scalable mechanisms for establishment of security associations between the NAS and home AAA server, such as provisioning of certificates. While this can be accommodated by use of RADIUS over IPsec, as specified in [RFC3579], this is not yet widely deployed. Given this, it does not appear practical at this time to define an equivalent re-direct mechanism within RADIUS and require its use with the attributes defined in this document.

Accordingly, the keying material included in the EAP-Master-Session-

Key attribute is encrypted on a hop-by-hop basis and is accessible to RADIUS proxies in the path. The security requirements defined in [Housley] can therefore only be satisfied if RADIUS clients are configured to talk directly to RADIUS servers without proxies.

8. References

8.1. Normative references

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

[RFC2865] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3394] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, September 2002.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[DiamEAP] Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-10.txt, Internet draft (work in progress), May 2005.

[KEYFRAME] Aboba, B., Simon, D., Arkko, J., Eronen, P. and H. Levkowetz, "EAP Key Management Framework", draft-ietf-eap-keying-06.txt, March 2005.

8.2. Informative references

[Housley] Housley, R. and B. Aboba, "AAA Key Management", draft-housley-aaa-key-mgmt-00.txt, Internet draft (work in progress), June 2005.

[IEEE-802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE-802.11] 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, IEEE Std. 802.11-2003, 2003.

[IEEE-802.1X]
IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, December 2004.

[IEEE-802.11i]
Institute of Electrical and Electronics Engineers, "Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE 802.11i, July 2004.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS", RFC 3575, July 2003.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G. and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J., "Diameter Base Protocol", RFC 3588, September 2003.

Acknowledgments

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

Authors' Addresses

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

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Open issues

Open issues relating to this specification are tracked on the following web site:

http://www.drizzle.com/~aboba/RADEXT/