Network Working Group William A. Arbaugh
INTERNET-DRAFT University of Maryland
Category: Experimental Bernard Aboba
<draft-irtf-aaaarch-handoff-01.txt> Microsoft
23 April 2003

Experimental Handoff Extension to RADIUS

Abstract

In order to decrease handoff latency, the concept of pre-emptive provisioning is under investigation. This document describes an experimental extension that enables an accounting server to notify a NAS of a prospective handoff. This enables the NAS to reserve resources and obtain the session parameters prior to arrival of the client, potentially reducing handoff times. The extension described in this document may potentially be useful in enabling handoffs across access technologies and providers. However, whether the approach described in this document is effective, deployable or secure is the subject of current research. It is offered for RADIUS primarily because source code for RADIUS client and server implementations is readily available for research purposes. Given that this extension represents research work in progress, implementation of this specification for purposes other than research is not recommended.

Table of Contents

1. Introduction

In wireless networks such as IEEE 802.11, described in [IEEE80211], it may be desirable to improve the speed at which handoff can be completed. Where RADIUS Accounting [RFC2866] is implemented, RADIUS Accounting packets will be generated each time the client connects to a NAS. Accounting packets from a single session, across multiple NASes, are uniquely identified by the Acct-Multi-Session-Id attribute, described in [RFC2866] and [Congdon].

The sequence of NASes contacted by clients as they move creates a graph representing the mobility paths of the clients. We call this graph a neighbor graph with NASes as the vertices and the mobility paths between the NASes as the edges. Thus, the number of neighbors for a given NAS is given by the degree function applied to the vertex representing the given NAS, e.g. for NAS_A the number of neighbors would be given by deg(v_A) where deg is the degree function deg: V -> int. Through knowledge of the neighbor graph, it is possible for a RADIUS server to anticipate client movements and provide advance notice of a potential handoff to the NAS. This advance notice, known as a Notify-Request in this specification, allows the NAS to reserve resources and obtain the session authorization parameters prior to arrival of the client. This removes the latency of the RADIUS exchange from the critical path for processing a handoff, decreasing handoff latency substantially, as described in [IEEE-02-758, IEEE-03-084]. Assuming that the coverage area is overlapping, this technique can support handoffs at vehicular velocities. The creation and maintenance of neighbor graphs at an authentication server is described in [Mishra]. An alternate approach to using neighbor graphs uses a matrix of probabilities and is described in [8021XHandoff].

By nature, client behavior is not completely predictable, so that the handoff advance notice is only advisory. The client identified in the advance notice may never contact the NAS, or may contact it long after the initial notice is received. As a result, the NAS will typically free reserved resources after a suitable waiting period, known as the Reservation-Lifetime. In situations where resources are at a premium, it may be desirable to minimize resources reserved for clients that are no longer likely to attempt to connect to a given NAS. To accomplish this, the reservation period can be shortened, or alternatively, the RADIUS server can remove resource reservations using the Disconnect-Request, specified in [DynAuth]. A client contacting the NAS after the Reservation-Lifetime has expired or a resource reservation has been removed will be unable to complete a handoff, and will need to do a fast resume, such as is supported in EAP TLS [RFC2716].

The extension described in this document enables a RADIUS Server to send Notify-Requests to NASes, and to receive Notify-Responses. The Notify-

Request identifies the session to be handed off and the NAS on which it currently resides. Attributes included within the Notify-Request are described in Section 2.1.

If the NAS has resources available to reserve, and if it is enabled to support this handoff extension, then it will respond with a Notify-Accept. If resources are not available (such as when previous resource commitments leave insufficient resources remaining), or if the NAS does not wish to support the prospective handoff for any other reason, the NAS will respond with a Notify-Reject, specifying the reason why the requested handoff reservation could not be carried out, using the Error-Cause attribute, specified in [DynAuth].

After the NAS responds with a Notify-Accept, it will typically issue an Access-Request to the RADIUS server. This allows the NAS to obtain the authorizations for the session before it is contacted by the client. The contents of the Access-Request sent by the NAS will depend on the form of access it is providing, so that it cannot be specified in detail here. However, for use with IEEE 802.11, it is expected that an Access-Request will be sent with a NAS-Port-Type=802.11 and a Service-Type=Handoff. For other access methods, a different NAS-Port-Type value might be sent, perhaps with a different value for Service-Type.

Since the extension defined in this document supports multiple access methods and service types, and leverages the conventional RADIUS Access-Request/Response exchange, it can be used to enable handoffs between any access technology compatible with RADIUS. For example, using this extension, it is possible to enable a handoff between 802.11 and cellular technologies such as GPRS or CDMA 1X-RTT. When this extension is used to enable handoff between heterogeneous technologies, the "correctness" issues described in [Context] do not arise, since the RADIUS server provides the authorizations appropriate for each NAS and access mechanism.

This extension can also enable handoffs between providers that do not establish mutual trust, as would be required when using a context transfer approach, such as [IEEE80211f]. All that is necessary is that each NAS be able to reach the home RADIUS server through an appropriate path. Of course, where handoffs occur across different providers and access media, it is unlikely that session continuity can be preserved, since the client will be likely to change its IP address.

1.1. Terminology

This document uses the following terms:

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.

Network Access Server (NAS)
The device providing access to the network.

Service
The NAS provides a service to the user, such as IEEE 802 or PPP.

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.

Session
Each service provided by the NAS to a user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A user may have multiple sessions in parallel or series if the NAS supports that, with each session generating a separate start and stop accounting record. Where the client is mobile and is able to handoff between NASes, multiple related sessions may be uniquely identified by the Acct-Multi-Session-Id attribute.

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. These words are often capitalized. 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. Packet format

Exactly one Notify-Request, Notify-Accept or Notify-Reject packet is encapsulated in the UDP Data field. For the Notify-Request packet, the UDP Destination Port field is TBD. When a reply is generated, the source and destination ports are reversed.

A summary of the data 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Code

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded. RADIUS codes (decimal) for this extension are assigned as follows:

TBD - Notify-Request
TBD - Notify-Accept
TBD - Notify-Reject

Identifier

The Identifier field is one octet, and aids in matching requests and replies. The RADIUS server can detect a duplicate request if it has the same client source IP address and source UDP port and Identifier within a short span of time.

Length

The Length field is two octets. It indicates the length of the

packet including the Code, Identifier, Length, Authenticator and Attribute fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the packet is shorter than the Length field indicates, it MUST be silently discarded. The minimum length is 20 and maximum length is 4096.

Authenticator

The Authenticator field is sixteen (16) octets. The most significant octet is transmitted first. This value is used to authenticate the messages between the client and RADIUS server.

Request Authenticator

In Notify-Request Packets, the Authenticator value is a 16 octet MD5 [RFC1321] checksum, called the Request Authenticator. The Request Authenticator is calculated the same way as for an Accounting-Request, specified in [RFC2866].

Note that the Request Authenticator of an Notify-Request can not be done the same way as the Request Authenticator of a RADIUS Access-Request, because there is no User-Password attribute in an Notify-Request.

Response Authenticator

The Authenticator field in a Notify-Accept or Notify-Reject packet is called the Response Authenticator, and contains a one-way MD5 hash calculated over a stream of octets consisting of the Notify-Response Code, Identifier, Length, the Request Authenticator field from the Notify-Request packet being replied to, and the response attributes if any, followed by the shared secret. The resulting 16 octet MD5 hash value is stored in the Authenticator field of the Notify-Accept or Notify-Reject packet.

Attributes

In Notify-Request messages, all attributes are treated as mandatory. A NAS MUST respond to a Notify-Request containing one or more unsupported attributes with a Notify-Reject. A Notify-Reject MUST NOT result in resources being reserved on the NAS. Attributes beyond those specified in Section 3 SHOULD NOT be included within Notify-Request messages, since this could produce unpredictable results.

When using a forwarding proxy, the proxy must be able to alter the packet as it passes through in each direction. When the proxy forwards a Notify-Request, it MAY add a Proxy-State Attribute, and when the proxy forwards a response, it MUST remove its Proxy-State

Attribute if it added one. Proxy-State is always added or removed after any other Proxy-States, but no other assumptions regarding its location within the list of attributes can be made. Since Notify responses are authenticated on the entire packet contents, the stripping of the Proxy-State attribute invalidates the integrity check - so the proxy needs to recompute it. A forwarding proxy MUST NOT modify existing Proxy-State, State, or Class attributes present in the packet.

If there are any Proxy-State attributes in a Notify-Request received from the server, the forwarding proxy MUST include those Proxy-State attributes in its response to the server. The forwarding proxy MAY include the Proxy-State attributes in the Notify-Request when it forwards the request, or it MAY omit them in the forwarded request. If the forwarding proxy omits the Proxy-State attributes in the request, it MUST attach them to the response before sending it to the server.

2.1. Notify-Request

Description

A Notify-Request packet is sent by the RADIUS server to the NAS to notify it of the potential handoff of a specified session.

Code

TBD - Notify-Request

Identifier

The Identifier field MUST be changed whenever the content of the Attributes field changes, and whenever a valid reply has been received for a previous request. For retransmissions where the contents are identical, the Identifier MUST remain unchanged.

Note that if the Event-Timestamp attribute is included the Notify-Request then the Event-Timestamp value will be updated when the packet is retransmitted, changing the content of the Attributes field and requiring a new Identifier and Request Authenticator.

Request Authenticator

The Request Authenticator of an Accounting-Request contains a 16-octet MD5 hash value calculated according to the method described in "Request Authenticator" in Section 2.

Attributes

The Attribute field is variable in length, and contains a list of Attributes. In Notify-Request packets, certain attributes are used to uniquely identify the NAS as well as a potential user session on the NAS, and to describe the services to be provided. All NAS identification attributes included in a Notify-Request message MUST match in order for a Notify-Accept to be sent; otherwise a Notify-Reject MUST be sent.
To address security concerns described in Section 4.1, the User-Name attributes MUST be present in Notify-Request packets. To address security concerns described in Section 4.2, the NAS-IP-Address and/or NAS-IPv6-Address attributes SHOULD be present in Notify-Request packets; the NAS-Identifier attribute MAY be present in addition. Details of the attributes which may be included in Notify-Request packets are provided in Section 3.

2.2. Notify-Accept

Description

The NAS responds to the Notify-Request with a Notify-Accept if the NAS agrees to to prepare for a handoff of the specified session.

Code

TBD - Notify-Accept

Identifier

The Identifier field is a copy of the Identifier field of the Notify-Request which caused this Notify-Accept.

Response Authenticator

The Response Authenticator of a Notify-Accept contains a 16-octet MD5 hash value calculated according to the method described in "Response Authenticator" in Section 2.

Attributes

The Attribute field is variable in length, and contains a list of Attributes. Within the Notify-Accept, attributes are used to provide the RADIUS server with the session identifiers that will be used by the NAS in subsequent Access-Request and Accounting-Request packets. This includes session identification attributes, such as the User-Name and Acct-Multi-Session-Id attributes provided by the RADIUS server in the Notify-Request, as well as an Acct-Session-Id allocated by the NAS for the handoff, should it occur. The Idle-Timeout attribute, when included in the Notify-Accept, provides the RADIUS

server with the time that the NAS is willing to reserve resources for the handoff. Section 3 provides more detail on the attributes permitted within the Notify-Accept packet.

2.3. Notify-Reject

Description

The NAS responds to the Notify-Request with a Notify-Reject if the NAS does not have the resources to make the required handoff preparations, or wishes to decline for any other reason.

Code

TBD - Notify-Reject

Identifier

The Identifier field is a copy of the Identifier field of the Notify-Request which caused this Notify-Reject.

Response Authenticator

The Response Authenticator of a Notify-Accept contains a 16-octet MD5 hash value calculated according to the method described in "Response Authenticator" in Section 2.

Attributes

The Attribute field is variable in length, and contains a list of Attributes. Within the Notify-Reject, the Error-Cause attribute provides the RADIUS server with the reason why the Notify-Request could not be honored. Values of the Error-Cause attribute, and their corresponding meanings are described in [DynAuth], Section 3.1.

3. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity. If an attribute is not mentioned in this table, then it SHOULD NOT be included in Notify-Request, Notify-Accept or Notify-Reject packets.

Notify Request	Notify Accept	Notify Reject	#	Attribute
1	1	0	1	User-Name [Note 1]
0-1	0	0	4	NAS-IP-Address [Note 2]
0-1	0	0	5	NAS-Port [Note 5]
1	0	0	6	Service-Type [Note 10,11]
0-1	0	0	7	Framed-Protocol [Note 10]
0-1	0-1	0	28	Idle-Timeout [Note 3]
0-1	0	0	30	Called-Station-Id [Note 4]
0-1	0	0	31	Calling-Station-Id [Note 1]
0-1	0	0	32	NAS-Identifier [Note 2]
0+	0+	0+	33	Proxy-State
0	0-1	0	44	Acct-Session-Id [Note 7]
0-1	0-1	0	50	Acct-Multi-Session-Id [Note 6]
0-1	0-1	0-1	55	Event-Timestamp [Note 9]
1	0	0	61	NAS-Port-Type [Note 10]
0-1	0	0	87	NAS-Port-Id [Note 5]
0-1	0	0	94	Originating-Line-Info [Note 5]
0-1	0	0	95	NAS-IPv6-Address [Note 2]
0	0	0-1	TBD	Error-Cause [Note 8]
Notify Request	Notify Accept	Notify Reject	#	Attribute

[Note 1] The User-Name attribute MUST be provided in the Notify-Request and MUST be echoed in the Notify-Accept, and subsequent Access-Request packets.

[Note 2] A Notify-Request MUST contain a NAS-IP-Address, NAS-IPv6-Address or NAS-Identifier attribute (or some combination of these).

[Note 3] Within a Notify-Request, the Idle-Timeout attribute provides a suggested amount of time for which the NAS may reserve resources for a potential handoff. If an Idle-Timeout attribute is included within the Notify-Request, then if the NAS is unable to reserve resources for this period of time, then it MUST include an Idle-Timeout attribute in the Notify-Accept, if sent, specifying the time it is willing to commit to. The RADIUS server should assume that the resources have been released at time Event-Timestamp + Idle-Timeout.

[Note 4] Within a Notify-Request, Called-Station-Id refers to the NAS from which the handoff is expected to occur. If the handoff does not occur from that NAS referred to in Called-Station-Id, then the NAS MAY refuse the handoff. In the case where NAS-Port-Type = 802.11, and the Called-Station-Id contains an SSID, then if the handoff occurs, the client MUST be granted access only to this SSID. If the attempts to connect to another SSID, then the NAS MUST deny network access to the client. If the SSID field is omitted, then a value of ANY is assumed.

[Note 5] The NAS-Port and NAS-Port-Id attributes, if present, refer to the NAS port from which the handoff is expected to occur. Originating-Line-Info provides information on how the session originated.

[Note 6] Within a Notify-Request, the Acct-Multi-Session-Id provides a unique identifier for user sessions during handoffs between NASes. The Acct-Multi-Session-Id is echoed in subsequent Access-Request and Accounting-Request packets.

[Note 7] The Acct-Session-Id, if present in Notify-Accept packets, denotes the accounting session id allocated by the NAS for the prospective handoff, should it occur. The Acct-Session-Id is echoed in subsequent Access-Request and Accounting-Request packets.

[Note 8] The Error-Cause attribute is present only in Notify-Reject packets, and specifies the reason for the rejection. It is defined in [DynAuth], Section 3.1.

[Note 9] When IPsec replay protection is not used, the Event-Timestamp attribute MUST be present in all packets in order to prevent replay attacks. This is discussed in Section 4.

[Note 10] The Service-Type, NAS-Port-Type, and Framed-Protocol attributes are used to specify the services that are to be provided to the handed off session. The Service-Type and NAS-Port-Type attributes MUST be present in the Notify-Request; when used with 802.11, it is expected that a NAS-Port-Type=802.11 and a Service-Type=Handoff will be included. The Service-Type is echoed in the subsequent Access-Request.

If the NAS is not able to provide the specified service, then it MUST send a Notify-Reject.

[Note 11] The Service-Type value of Handoff, when used by the NAS in an Access-Request packet, indicates that a handoff request is being anticipated and that the RADIUS server should send back an Access-Accept to allow the prospective handoff to occur, or an Access-Reject to deny the prospective handoff. The decision is typically based on the User-Name, Called-Station-Id or Calling-Station-Id. As with a normal Access-Request, the User-Name attribute is expected to be filled in. Note that the service provided when Service-Type=Handof differs from that provided when Service-Type=Call Check. With Handoff, the NAS MUST authenticate the user during the handoff prior to allowing access, using credentials provided by the RADIUS server, whereas with a Service-Type=Call Check, the authentication is implicit and access is permitted or denied purely based on the Called-Station-Id or Calling-Station-Id.

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 packet.
0-1   Zero or one instance of this attribute MAY be present in packet.
1   Exactly one instance of this attribute MUST be present in packet.

4. Security considerations

4.1. Authorization issues

Where a NAS is shared by multiple providers, it is undesirable for one provider to be able to send Notify-Requests relating to sessions of another provider.

To prevent this, the RADIUS proxy SHOULD perform a "reverse path forwarding" (RPF) check to verify that a Notify-Request is originating from an authorized RADIUS server. In a network model where a proxy is employed to forward Notify-Request messages, the NAS MUST accept these messages only from proxies that it is configured to trust. Requests from untrusted sources MUST be silently discarded.

To perform the RPF check, the proxy uses the session identification attributes included in Notify-Request messages, in order to determine the RADIUS server(s) to which an equivalent Access-Request would be routed. If this matches the source address of the Notify-Request, then the Request is forwarded; otherwise it SHOULD be silently discarded.

Typically the proxy will extract the realm from the Network Access Identifier [RFC2486] included within the User-Name attribute, and determine the corresponding RADIUS servers in the proxy routing tables. The RADIUS servers for that realm are then compared against the source address of the packet. Where no RADIUS proxy is present, the RPF check will need to be performed by the NAS itself.

Since authorization to send a Notify-Request is determined based on the source address and the corresponding shared secret, the NASes or proxies SHOULD configure a different shared secret for each RADIUS server.

4.2. Impersonation

[RFC2865] Section 3 states:

> A RADIUS server MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that RADIUS requests can be proxied.

When RADIUS requests are forwarded by a proxy, the NAS-IP-Address or NAS-IPv6-Address attributes will typically not match the source address observed by the RADIUS server. Since the NAS-Identifier attribute need not contain an FQDN, this attribute may not be resolvable to the source

address observed by the RADIUS server, even when no proxy is present.

As a result, the authenticity check performed by a RADIUS server or proxy does not verify the correctness of NAS identification attributes. This makes it possible for a rogue NAS to forge NAS-IP-Address, NAS-IPv6-Address or NAS-Identifier attributes within a RADIUS Access-Request in order to impersonate another NAS. It is also possible for a rogue NAS to forge session identification attributes such as the Called-Station-Id, Calling-Station-Id, or Originating-Line-Info. This could fool the RADIUS server into sending Notify-Request messages containing forged session identification attributes to a NAS targeted by an attacker.

To address these vulnerabilities RADIUS proxies SHOULD check whether NAS identification attributes match the source address of packets originating from the NAS. Where one or more attributes do not match, Notify-Request messages SHOULD be silently discarded.

Such a check may not always be possible. Since the NAS-Identifier attribute need not correspond to an FQDN, it may not be resolvable to an IP address to be matched against the source address. Also, where a NAT exists between the RADIUS client and proxy, checking the NAS-IP-Address or NAS-IPv6-Address attributes may not be feasible.

4.3. IPsec usage guidelines

Implementations of this specification SHOULD support IPsec [RFC2401] along with IKE [RFC2409] for key management. IPsec ESP [RFC2406] with non-null transform SHOULD be supported, and IPsec ESP with a non-null encryption transform and authentication support SHOULD be used to provide per-packet confidentiality, authentication, integrity and replay protection. IKE SHOULD be used for key management.

Within RADIUS [RFC2865], a shared secret is used for hiding of attributes such as User-Password, as well as in computation of the Response Authenticator. In RADIUS accounting [RFC2866], the shared secret is used in computation of both the Request Authenticator and the Response Authenticator.

Since in RADIUS a shared secret is used to provide confidentiality as well as integrity protection and authentication, only use of IPsec ESP with a non-null transform can provide security services sufficient to substitute for RADIUS application-layer security. Therefore, where IPsec AH or ESP null is used, it will typically still be necessary to configure a RADIUS shared secret.

Where RADIUS is run over IPsec ESP with a non-null transform, the secret shared between the NAS and the RADIUS server MAY NOT be configured. In

this case, a shared secret of zero length MUST be assumed. However, a RADIUS server that cannot know whether incoming traffic is IPsec-protected MUST be configured with a non-null RADIUS shared secret.

When IPsec ESP is used with RADIUS, DES-CBC SHOULD NOT be used as the encryption transform, and per-packet authentication, integrity and replay protection MUST be used. A typical IPsec policy for an IPsec-capable RADIUS client is "Initiate IPsec, from me to any destination port UDP 1812".

This causes an IPsec SA to be set up by the RADIUS client prior to sending RADIUS traffic. If some RADIUS servers contacted by the client do not support IPsec, then a more granular policy will be required: "Initiate IPsec, from me to IPsec-Capable-RADIUS-Server, destination port UDP 1812".

For a client implementing this specification the policy would be "Accept IPsec, from any to me, destination port UDP TBD". This causes the RADIUS client to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all RADIUS servers connecting to an IPsec-enabled RADIUS client, since some RADIUS servers may not support IPsec.

For an IPsec-capable RADIUS server, a typical IPsec policy is "Accept IPsec, from any to me, destination port 1812". This causes the RADIUS server to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all RADIUS clients connecting to an IPsec-enabled RADIUS server, since some RADIUS clients may not support IPsec.

For servers implementing this specification, the policy would be "Initiate IPsec, from me to any, destination port UDP TBD". This causes the RADIUS server to initiate IPsec when sending RADIUS extension traffic to any RADIUS client. If some RADIUS clients contacted by the server do not support IPsec, then a more granular policy will be required, such as "Initiate IPsec, from me to IPsec-capable-RADIUS-client, destination port UDP TBD".

Where IPsec is used for security, and no RADIUS shared secret is configured, it is important that trust be demonstrated between the RADIUS client and RADIUS server by some means. For example, before enabling an IKE-authenticated host to act as a RADIUS client, the RADIUS server SHOULD check whether the host is authorized to provide network access. Similarly, before enabling an IKE-authenticated host to act as a RADIUS server, the RADIUS client SHOULD check whether the host is authorized for that role.

RADIUS servers can be configured with the IP addresses (for IKE Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of RADIUS clients. Alternatively, if a separate Certificate Authority (CA) exists for RADIUS clients, then the RADIUS server can configure this CA as a trust anchor [RFC3280] for use with IPsec.

Similarly, RADIUS clients can be configured with the IP addresses (for IKE Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of RADIUS servers. Alternatively, if a separate CA exists for RADIUS servers, then the RADIUS client can configure this CA as a trust anchor for use with IPsec.

Since unlike SSL/TLS, IKE does not permit certificate policies to be set on a per-port basis, certificate policies need to apply to all uses of IPsec on RADIUS clients and servers. In IPsec deployment supporting only certificate authentication, a management station initiating an IPsec-protected telnet session to the RADIUS server would need to obtain a certificate chaining to the RADIUS client CA. Issuing such a certificate might not be appropriate if the management station was not authorized as a RADIUS client.

Where RADIUS clients may obtain their IP address dynamically (such as an Access Point supporting DHCP), Main Mode with pre-shared keys [RFC2409] SHOULD NOT be used, since this requires use of a group pre-shared key; instead, Aggressive Mode SHOULD be used. Where RADIUS client addresses are statically assigned either Aggressive Mode or Main Mode MAY be used. With certificate authentication, Main Mode SHOULD be used.

Care needs to be taken with IKE Phase 1 Identity Payload selection in order to enable mapping of identities to pre-shared keys even with Aggressive Mode. Where the ID_IPV4_ADDR or ID_IPV6_ADDR Identity Payloads are used and addresses are dynamically assigned, mapping of identities to keys is not possible, so that group pre-shared keys are still a practical necessity. As a result, the ID_FQDN identity payload SHOULD be employed in situations where Aggressive mode is utilized along with pre-shared keys and IP addresses are dynamically assigned. This approach also has other advantages, since it allows the RADIUS server and client to configure themselves based on the fully qualified domain name of their peers.

Note that with IPsec, security services are negotiated at the granularity of an IPsec SA, so that RADIUS exchanges requiring a set of security services different from those negotiated with existing IPsec SAs will need to negotiate a new IPsec SA. Separate IPsec SAs are also advisable where quality of service considerations dictate different handling RADIUS conversations. Attempting to apply different quality of service to connections handled by the same IPsec SA can result in

reordering, and falling outside the replay window. For a discussion of the issues, see [RFC2983].

4.4. Replay protection

Since this specification utilizes the Request Authenticator field for integrity protection and authentication, rather than as a nonce, no liveness or protection against replay is provided by the RADIUS header.

Where IPsec replay protection is not used, in order to provide replay protection, the Event-Timestamp (55) attribute, described in [RFC2869] MUST be included in all messages. When this attribute is present, the RADIUS server MUST check that the Event-Timestamp is current within an acceptable time window. This implies the need for time synchronization within the network, which can be achieved via a variety of mechanisms, including secure NTP, as described in [NTPAuth]. Both the NAS and the RADIUS server SHOULD be configurable to silently discard messages lacking an Event-Timestamp attribute. A default time window of 300 seconds is recommended.

4.5. Spoofing and hijacking

Access-Request packets with a User-Password attribute establish the identity of both the user and the NAS sending the Access-Request, because of the way the shared secret between the NAS and RADIUS server is used. Access-Request packets with CHAP-Password or EAP-Message attributes do not have a User-Password attribute. As a result, the Message-Authenticator attribute SHOULD be used in Access-Request packets that do not have a User-Password attribute, in order to establish the identity of the NAS sending the request. This includes Access-Request packets with a Service-Type attribute with a value of Handoff.

An attacker may attempt to inject packets into the conversation between the NAS and the RADIUS server. RADIUS [RFC2865] does not support encryption other than attribute hiding. As described in [RFC2865], only Access-Reply and Access-Challenge packets are authenticated and integrity protected. Moreover, the per-packet authentication and integrity protection mechanism described in this specification has known weaknesses [MD5Attack], making it a tempting target for attackers.

To provide stronger security, implementations of this specification SHOULD use IPsec ESP with non-null transform and per-packet encryption, authentication, integrity and replay protection.

5. IANA Considerations

This specification requires assignment a UDP port, in addition to RADIUS Type codes for Notify-Request, Notify-Accept, and Notify-Reject. A new

value is requested to be allocated for the Service-Type attribute for Handoff.

6. Normative references

[RFC1305] Mills, D. L., "Network Time Protocol (version 3) Specification, Implementation and Analysis, RFC 1305 March, 1992.

[RFC1321] Rivest, R., Dusse, S., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

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

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

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

[RFC2869] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

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

[IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[Congdon] Congdon, P., et al., "IEEE 802.1X RADIUS Usage Guidelines", Internet draft (work in progress), draft-congdon-radius-8021x-29.txt, April 2003.

[DynAuth] Chiba, M., et. al., "Dynamic Authorization Extensions to Remote Authentication Dial-in User Service (RADIUS)", Internet draft (work in progress), draft-chiba-radius-dynamic-authorization-18.txt, April 2003.

7. Informative references

[Mishra] Mishra, A., Shin, M., Arbaugh, W., Lee, I. and K. Jang, "Experimental Neighbor Graph Creation and Maintenance", Internet draft (work in progress), draft-irtf-aaaarch-neighbor-graph-00.txt.

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

[RFC2434] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

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

[RFC2716] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[RFC2983] Black, D. "Differentiated Services and Tunnels", RFC 2983, October 2000.

[Context] Aboba, B. and T. Moore, "A Model for Context Transfer in IEEE 802", draft-aboba-802-context-02.txt, Internet draft (work in progress), April 2002.

[IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE8021Q] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q, January 1998.

[IEEE-02-758] Mishra, A., Shin, M., Arbaugh, W., Lee, I. and K. Jang, "Proactive Caching Strategies for IAPP Latency Improvement during 802.11 Handoff", IEEE 802.11 Working Group, IEEE-02-758r1-F, November 2002.

[IEEE-03-084] Mishra, A., Shin, M., Arbaugh, W., Lee, I. and K. Jang, "Proactive Key Distribution to support fast and secure roaming", IEEE 802.11 Working Group, IEEE-03-084r1-I, http://www.ieee802.org/11/Documents/DocumentHolder/ 3-084.zip, January 2003.

[8021XHandoff] Pack, S. and Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1X Model", School of Computer Science and Engineering, Seoul National University, Seoul, Korea, 2002.

[IEEE8023] ISO/IEC 8802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3-1996), 1996.

[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, IEEE Std. 802.11-1999, 1999.

[IEEE80211f] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE Draft 802.11f/D5, January 2003.

[MD5Attack] Dobbertin, H., "The Status of MD5 After a Recent Attack." CryptoBytes Vol.2 No.2, Summer 1996.

[NASREQ] Calhoun, P., et al., "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-11.txt, Internet draft (work in progress), February 2003.

[NTPAuth] Mills, D., "Public Key Cryptography for the Network Time Protocol", Internet draft (work in progress), draft-ietf-stime-ntpauth-05.txt, November 2002.

Acknowledgments

The authors would like to acknowledge the following people for contributions to this document: Tim Moore (Microsoft), Min-ho Shin (University of Maryland), Nick Petroni (University of Maryland), Adam Sulmicki (University of Maryland), Insun Lee (Samsung Electronics), Kyunghun Jang (Samsung Electronics).

Authors' Addresses

William A. Arbaugh
Department of Computer Science
University of Maryland, College Park
A.V. Williams Building
College Park, MD 20742

EMail: waa@cs.umd.edu
Phone: +1 301 405 2774

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

Expiration Date

This memo is filed as <draft-irtf-aaaarch-handoff-01.txt>, and expires November 22, 2003.