Network Working Group
INTERNET-DRAFT
Updates: 5176
Category: Standards Track
<draft-ietf-radext-coa-proxy-04.txt>
24 April 2018

DeKok, Alan
FreeRADIUS
J. Korhonen
Nokia Siemens Networks

Dynamic Authorization Proxying in Remote Authorization Dial-In User Service Protocol (RADIUS) draft-ietf-radext-coa-proxy-04.txt

Abstract

RFC 5176 defines Change of Authorization (CoA) and Disconnect Message (DM) behavior for RADIUS. Section 3.1 of that document suggests that proxying these messages is possible, but gives no guidance as to how that is done. This specification corrects that omission for scenarios where networks use Realm-based proxying as defined in [RFC7542].

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

RFC 5176 [RFC5176] defines Change of Authorization (CoA) and Disconnect Message (DM) behavior for RADIUS. Section 3.1 of that document suggests that proxying these messages is possible, but gives no guidance as to how that is done. This omission means that in practice, proxying of CoA packets is impossible.

We correct that ommission here by explaining how proxying of these packets can be done by leveraging an existing RADIUS attribute, Operator-Name (Section 4.1 of [RFC5580]). We then explain how this attribute can be used by CoA proxies to route packets "backwards" through a RADIUS proxy chain to the Visited Network. We introduce a new attribute; Operator-NAS-Identifier, which permits packets to be routed from the RADIUS server at the Visited Network to the NAS. We then explain how use of this attribute can increase privacy of the internal implementation of the visited network.

We limit the use-case of CoA proxying to Realm-based proxying as defined in [RFC7542]. Other forms of CoA proxying are possible, but are not specified here.

We conclude with a discussion of the security implications of the design, and show how they are acceptable.

1.1. Terminology

This document frequently uses the following terms:

CoA

Change of Authorization, e.g. CoA-Request, or CoA-ACK, or CoA-NAK, as defined in [RFC5176]. That specification also defines Disconnect-Request, Disconnect-ACK, and Disconnect-NAK. For simplicity here, where we use "CoA", we mean a generic "CoA-Request or Disconnect-Request" packet. We use "CoA-Request" or "Disconnect-Request" to refer to the specific packet types.

Network Access Identifier

The Network Access Identifier (NAI) [RFC7542] is the user identity submitted by the client during network access authentication. The purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request. Please note that the NAI may not necessarily be the same as the user's email address or the user identity submitted in an application layer authentication.

Network Access Server

The Network Access Server (NAS) is the device that clients connect to in order to get access to the network. In PPTP terminology, this is referred to as the PPTP Access Concentrator (PAC), and in L2TP terminology, it is referred to as the L2TP Access Concentrator (LAC). In IEEE 802.11, it is referred to as an Access Point.

Home Network

The network which holds the authentication credentials for a user.

Visited Network

A network other than the home network, where the user attempts to gain network access. The Visited Network typically has a relationship with the Home Network, possibly through one or more intermediary proxies.

1.2. Requirements Language

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. Problem Statement

This section describes how RADIUS proxying works, how CoA packets work, and why CoA proxying as discussed in RFC 5176 is insufficient in practice.

2.1. Typical RADIUS Proxying

When a RADIUS server proxies an Access-Request packet, it typically does so based on the contents of the User-Name attribute, which contains a Network Access Identifier [RFC7542]. Other methods are possible, but we restrict ourselves to this usage, as it is the most common one.

The proxy server looks up the "Realm" portion of the NAI in a logical AAA routing table, as described in Section 3 of [RFC7542]. The entry in that table is the "next hop" to which the packet is sent. This "next hop" may be another proxy, or it may be the home server for that realm.

If the "next hop" is a proxy, it will perform the same Realm lookup, and then proxy the packet. Alternatively, if the "next hop" is the Home Server for that realm, it will try to authenticate the user, and respond with an Access-Accept, Access-Reject, or Access-Challenge.

The RADIUS client will match the response packet to an outstanding request. If the client is part of a proxy, it will then proxy that response packet in turn to the system which originated the Access-Request. This process occurs until the response packet arrives at the NAS.

The proxies are typically stateful with respect to ongoing request / response packets, but stateless with respect to user sessions. Once a response has been received by the proxy, it can discard all information about the request packet.

The same proxy method is used for Accounting-Request packets. The combination of the two methods allows proxies to connect Visited Networks to Home Networks for all AAA purposes.

2.2. CoA Processing

[RFC5176] describes how CoA clients send packets to CoA servers. We note that system comprising the CoA client is typically co-located with, or is the same as, the RADIUS server. Similarly, the CoA server is a system that is either co-located with, or is the same as, the RADIUS client.

In the case of packets sent inside of one network, the source and destination of CoA packets is locally determined. There is thus no need for standardization of that process, as networks are free to send CoA packets whenever they want, for whatever reason they want.

2.3. Failure of CoA Proxying

The situation is more complicated when multiple networks are involved. [RFC5176] suggests that CoA proxying is permitted, but makes no suggestions for how it should be done.

If proxies tracked user sessions, it might be possible for a proxy to match an incoming CoA-Request to a user session, and then to proxy that packet to the RADIUS client which originated the Access-Request for that sessions.

There are many problems with such a scenario. The CoA server may, in fact, not be co-located with the RADIUS client. The RADIUS client may be down, but there may be a different CoA server which could accept the packet. User session tracking can be expensive and complicated for a proxy, and many proxies do not record user sessions. Finally, [RFC5176] is silent on the topic of "session identification attributes", which makes it impossible for a proxy to determine if a CoA packet matches a particular user session.

The result of all of these issues is that CoA proxying cannot be performed when using the behavior defined in [RFC5176].

3. How to Perform CoA Proxying

The solution to the above problem is to use the Operator-Name attribute defined in [RFC5580], Section 4.1. We repeat a portion of that definition here for clarity:

> This attribute carries the operator namespace identifier and the operator name. The operator name is combined with the namespace identifier to uniquely identify the owner of an access network.

Followed by a description of the REALM namespace:

> REALM ('1' (0x31)):
>
> The REALM operator namespace can be used to indicate operator names based on any registered domain name. Such names are required to be unique, and the rights to use a given realm name are obtained coincident with acquiring the rights to use a particular Fully Qualified Domain Name (FQDN). ...

In short, the Operator-Name attribute contains the an ASCII "1", followed by the Realm of the Visited Network. e.g. for the "example.com" realm, the Operator-Name attribute contains the text "1example.com". This information is precisely what is needed by intermediate nodes, in order to perform CoA proxying.

3.1. Changes to Access-Request and Accounting-Request packets

When a Visited Network proxies an Access-Request or Accounting-Request packet outside of its network, it SHOULD include an Operator-Name attribute in the packet, as discussed in Section 4.1 of [RFC5580]. The contents of the Operator-Name should be "1", followed by the realm name of the Visited Network. Where the Visited Network has more than one realm name, a "canonical" one should be chosen, and used for all packets.

Visited Networks MUST use a consistent value for Operator-Name for one user session. That is, sending "1example.com" in an Access-Request packet, and "1example.org" in an Accounting-Request packet for that same session is forbidden. Such behavior would make it look like the users session was simultaneously in two different Visited Networks, which is impossible.

Proxies which record user session information SHOULD also record Operator-Name. Proxies which do not record user session information do not need to record Operator-Name.

Home Networks SHOULD record Operator-Name along with any other information that they record about user sessions. Home Networks which expect to send CoA packets to Visited Networks MUST record Operator-Name for each user session which originates from a Visited Network. Failure to record the Operator-Name would mean that it would be impossible to send CoA packets to the Visited Network.

Networks which contain both the RADIUS client and RADIUS server do not need to create, record or track Operator-Name. That is, if the Visited Network and Home Network are the same, there is no need to use the Operator-Name attribute.

3.2. Proxying of CoA-Request and Disconnect-Request packets

When a Home Network wishes to send a CoA-Request or Disconnect-Request packet to a Visited Network, it MUST include an Operator-Name attribute in the packet. The value of the Operator-Name MUST be the value which was recorded earlier for that user session.

The Home Network MUST lookup the realm from the Operator-Name in a logical "realm routing table", as discussed in [RFC7542] Section 3.

That logical realm table is defined there as:

> a logical AAA routing table, where the "utf8-realm" portion acts as a key, and the values stored in the table are one or more "next hop" AAA servers.

In order to support proxying of CoA packets, this table is extended to include a mapping between "utf8-realm" and one ore more "next hop" CoA servers.

When proxying CoA-Request and Disconnect-Request packets, the lookups will return data from the "CoA server" field, instead of the "AAA server" field.

In practice, this process means that CoA proxying works exactly like "normal" RADIUS proxying, except that the proxy decision is made using the realm from the Operator-Name attribute, instead of using the realm from the User-Name attribute.

Proxies which receive the CoA packet MUST look up the realm from the Operator-Name in a logical "realm routing table", as with Home Servers, above. The packet is then sent to the realm which was found in that table. This process continues with any subsequent proxies until the packet reaches the Visited Network.

The Visited Network can then send the CoA packet to the NAS, and return any response packet back up the proxy chain to the Home Server.

The only missing piece here is how the Visited Network gets the packet from its CoA server to the NAS. The Visited Network could use NAS-Identifier, NAS-IP-Address, or NAS-IPv6-Address, but these attributes may be incorrect, or may be missing entirely.

These attributes may be incorrect because proxies which forward Access-Request packets often re-write them for internal policy reasons. These attributes may be missing, because the Visited Network may not want all upstream proxies and Home Servers to have detailed information about the internals of its private network.

We therefore need a way to identifier a NAS in the Visited Network, in a way which is both private, and which does not use any existing attribute.

3.3. Operator-NAS-Identifier

The Operator-NAS-Identifier attribute contains opaque information which identifies a NAS in a Visited Network. It MAY appear in the

following packets: Access-Request, Accounting-Request, CoA-Request, or Disconnect-Request. Operator-NAS-Identifier MUST NOT appear in any other packet.

Operator-NAS-Identifier MAY occur in a packet if the packet also contains an Operator-Name attribute. Operator-NAS-Identifier MUST NOT appear in a packet if there is no Operator-Name in the packet. Operator-NAS-Identifier MUST NOT occur more than once in a packet.

An Operator-NAS-Identifer attribute SHOULD be added to an Access-Request or Accounting-Request packet by a Visited Network just before proxying a packet to an external RADIUS server. When the Operator-NAS-Identifer attribute is added to a packet, the following attributes MUST be deleted: NAS-IP-Address, NAS-IPv6-Address, NAS-Identifier. The proxy MUST then add a NAS-Identifier attribute, in order satisfy the requirements of Section 4.1 of [RFC2865], and of [RFC2866].

We suggest that the contents of the NAS-Identifier be the Realm name of the Visited Network. That is, for everyone outside of the Visited Network, there is only one NAS: the Visited Network itself. For the Visited Network, the identity of the NAS is private information, which is opaque to everyone else.

Description

An opaque token describing the NAS a user has logged into.

Type

TBD. To be assigned by IANA from the "short extended space".

Length

4 to 23.

Implementations supporting this attribute MUST be able to handle between one (1) and twenty (20) octets of data. Implementations creating an Operator-NAS-Identifier MUST NOT create attributes with more than twenty octets of data. A twenty octet string is more than sufficient to individually address all of the NASes on the planet.

Data Type

string. See [RFC8044] Section 3.6 for a definition.

Value

The contents of this attribute are an opaque token interpretable only by the Visited Network.

This token MUST allow the Visited Network to direct the packet to the NAS for the users session. In practice, this requirement means that the Visited Network will either track these tokens in a database, or it will create tokens which can be decoded in order to reveal the identity of the NAS.

4. Requirements

4.1. Requirements on Home Servers

The Operator-NAS-Identifier attribute MUST be stored by a Home Server along with any user session identification attributes. When sending a CoA packet for a user session, the Home Server MUST include any Operator-NAS-Identifier it has recorded for that session.

A Home Server MUST NOT send CoA packets for users of other networks. The provisions of the next few sections describe how other participants in the RADIUS ecosystem can enforce this requirement.

4.2. Requirements on Visited Networks

A Visited Network which receives a proxied CoA packet MUST perform all of the checks discussed above for proxies. This requirement is because we assume that the Visited Network has a proxy in between the NAS and any external (i.e. third-party) proxy. Situations where a NAS sends packets directly to a third-party RADIUS server are outside of the scope of this specification.

Due to the limited number of attributes allowed in CoA packets by [RFC5176] Section 2.3, a Visited Network MUST remove the Operator-Name and Operator-NAS-Identifier attributes from any CoA-Request or Disconnect-Request packet prior to proxying that packet to the final CoA server (i.e. NAS). This requirement is phrase more generically below, in Section 4.3.2.

A Visited Network may create an Operator-NAS-Identifier via many methods. The value SHOULD be cryptographically strong, and SHOULD be verifiable by the Visited Network, without requiring it to track every individual value of Operator-NAS-identifier in a database.

Exactly how this requirement is implemented is outside of the scope of this document.

4.3. Requirements on Proxies

There are a number of requirements on proxies, both CoA proxies and RADIUS proxies. For the purpose of this section, we assume that each RADIUS proxy shares a common administration with a corresponding CoA proxy, and that the two systems can communicate electronically. There is no requirement that these systems are co-located.

4.3.1. Security Requirements on Proxies

Section 6.1 of [RFC5176] has some security requirements on proxies which handle CoA-Request and Disconnect-Request packets:

> ... a proxy MAY perform a "reverse path forwarding" (RPF) check to verify that a Disconnect-Request or CoA-Request originates from an authorized Dynamic Authorization Client.

We strengthen that requirement by saying that a proxy MUST perform a "reverse path forwarding" (RPF) check to verify that a Disconnect-Request or CoA-Request originates from an authorized Dynamic Authorization Client. Without this check, a proxy may forward forged packets, and thus contribute to the forgery problem instead of preventing it.

Proxies which record user session information SHOULD verify the contents of a received CoA packet against the recorded data for that user session. If the proxy determines that the information in the packet does not match the recorded user session, it SHOULD return a CoA-NAK or Disconnect-NAK packet, which contains an Error-Cause attribute having value 503 ("Session Context Not Found").

We recognize that because a RADIUS proxy will see Access-Request and Accounting-Request packets, it will have sufficient information to forge CoA packets. The RADIUS proxy will thus have the ability to subsequently disconnect any user who was authenticated through itself.

We suggest that the real-world effect of this security problem is minimal. RADIUS proxies can already return Access-Accept or Access-Reject for Access-Request packets, and can change authorization attributes contained in an Access-Accept. Allowing a proxy to change (or disconnect) a user session post-authentication is not substantially different from changing (or refusing to connect) a user session during the initial process of authentiction.

The largest problem is that there are no provisions in RADIUS for "end to end" security. That is, the Visited Network and Home Network

cannot communicate privately in the presence of proxies. This limitation originates from the design of RADIUS for Access-Request and Accounting-Request packets. That limitation is then carried over to CoA-Request and Disconnect-Request packets.

We cannot therefore prevent proxies or Home Servers from forging CoA packets. We can only create scenarios where that forgery is hard to perform, and/or is likely to be detected.

4.3.2. Filtering Requirements on Proxies

Section 2.3 of [RFC5176] makes the following requirement for CoA servers:

> In CoA-Request and Disconnect-Request packets, all attributes MUST be treated as mandatory.

These requirements are too stringent for a CoA proxy. Instead, we say that for a CoA proxy, all attributes MUST NOT be treated as mandatory. Proxies SHOULD perform proxying based on Operator-Name, though other schemes are possible, but are not discussed here. Proxies SHOULD forward all packets as-is, with minimal changes. Only the final CoA server (i.e NAS) can make a decision on which attributes are mandatory and which are not.

Where Operator-Realm and Operator-NAS-Identifier is received by a proxy, the proxy MUST pass those attributes through unchanged. This requirement applies to all proxies, including ones which forward any or all of Access-Request, Accounting-Request, CoA-Request, and Disconnect-Request packets.

All attributes added by a RADIUS proxy when sending packets from the Visited Network to the Home Network Network MUST be removed by the corresponding CoA proxy from packets which travel the reverse path. That is, any attribute editing which is done on the "forward" path MUST be undone on the "reverse" path.

The result is that a NAS will only ever receive CoA packets which either contain attributes sent by the NAS to it's local RADIUS server, or contain attributes which are sent by the Home Server in order to perform a change of authorization.

We note that the above requirement applies not only to Operator-Name and Operator-NAS-Identifier, but also to any future attributes which are added by a RADIUS proxy.

5. Functionality

This section describes how the two attributes work together to permit CoA proxying.

5.1. User Login

In this scenario, we follow a roaming user attempting authentication in a Visited Network. The login attempt is done via a NAS in the Visited Network. That NAS will send an Access-Request packet to the visited RADIUS server. The visited RADIUS server will see that the user is roaming, and xwill add an Operator-Name attribute, with value "1" followed by it's own realm name. e.g. "1example.com". The visited RADIUS server MAY also add an Operator-NAS-Identifier.

The visited RADIUS server will then proxy the authentication request to an upstream server. That server may be the Home Server, or it may be a proxy. In the case of a proxy, the proxy will forward the packet, until the packet reaches the Home Server.

The Home Server will record both Operator-Name and Operator-NAS-Identfier along with other information about the users session.

5.2. CoA Proxing

When the Home Server determines that a user should be disconnecte, it looks up the Operator-Name and Operator-NAS-Identifer, along with other user session identifiers as described in [RFC5176]. The Home Server then looks up the realm from the Operator-Name attribute in the logical AAA routing table, in order to find the CoA server for that realm (which may be a proxy). The Disconnect-Request is then sent to that CoA server.

The CoA server receives the request, and if it is a proxy, performs a similar lookup as done by the Home Server. The packet is then proxied repeatedly until it reaches the Visited Network.

If the proxy cannot find a destination for the request, or if no Operator-Name attribute exists in the request, the proxy will return a CoA-NAK with Error-Cause 502 (Request Not Routable).

The Visited Network will recieve the CoA-Request packet, and will use the Operator-NAS-Identifier (if available) attribute to determine which local CoA server (i.e. NAS) the packet should be sent to. If there is no Opertor-NAS-Identifier attribute, the Visited Network may use other means to locate the NAS, such as consulting a local database which tracks user sessions.

The Operator-Name and Operator-NAS-Identifer attributes are then removed fromt he packet, and it is then sent to the CoA server.

If no CoA server can be found, the Visited Network return a CoA-NAK with Error-Cause 403 (NAS Identification Mismatch).

Any response from the CoA server (NAS) is returned to the Home Network, via the normal method of returning responses to requests.

6. Security Considerations

This specification incorporates by reference the [RFC6929] Section 11. In short, RADIUS has many known issues which are discussed in detail there, and which do not need to be repeated here.

This specification adds one new attribute, and defines new behavior for RADIUS proxying. As this behavior mirrors existing RADIUS proxying, we do not believe that it introduces any new security issues.

The Operator-NAS-Identifier SHOULD be created by the Visited Network such that its contents are opaque to all other parties. This ensures that anyone observing unencrypted RADIUS traffic gains no information about the internals of the Visited Network.

7. IANA Considerations

IANA is instructed to allocate one new RADIUS attribute, as per Section 3.3, above.

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

[RFC5580]
Tschofenig H., Ed. "Carrying Location Objects in RADIUS and Diameter", RFC 5580, August 2009.

[RFC6929]
DeKok A. and Lior, A., "Remote Authentication Dial-In User Service

(RADIUS) Protocol Extensions", RFC 6929, April 2013.

[RFC7542]
DeKok A., "The Network Access Identifier", RFC 7542, May 2015.

[RFC8044]
DeKok A., "Data Types in the Remote Authentication Dial-In User Service Protocol (RADIUS)", RFC 8044, January 2017.

8.2. Informative References

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

[RFC5176]
Chiba, M. et al, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

Authors' Addresses

Alan DeKok
The FreeRADIUS Server Project

Email: aland@freeradius.org

Jouni Korhonen

EMail: jouni.nospam@gmail.com