Network Working Group
Internet-Draft
Expires: April 25, 2005

F. Adrangi
Intel
A. Lior
Bridgewater Systems
J. Korhonen
Teliasonera

October 25, 2004

Chargeable User Identity
draft-adrangi-radius-chargeable-user-identity-02

Status of this Memo

Copyright Notice

Abstract

This document describes a new RADIUS attribute used by a home RADIUS to indicate Chargeable User Identity to all parties involved in the roaming transaction outside the home network.

Table of Contents

1. Introduction 3
1.1 Terminology 4
2. Operation 4
2.1 Chargeable User Identity Attribute (CUI) 4
3. Diameter RADIUS Interoperability 7
4. IANA Considerations 7
5. Security considerations 7
6. Acknowledgements 7
7. References 8
7.1 Normative references 8
7.2 Informative references 8
Authors' Addresses 9
Intellectual Property and Copyright Statements 10

1. Introduction

In certain authentication methods such as, EAP-PEAP or EAP-TTLS, EAP-SIM, and EAP-AKA, the true identity of the subscriber can be hidden from the RADIUS AAA servers outside the subscriberÆs home network. In these methods the UserName(1) attribute contains an anonymous identity (e.g., @example.com) sufficient to route the RADIUS packets to the home network but otherwise insufficient to identify the subscriber. While this mechanism is good practice there could be problems. Because Local and intermediate networks may require a user identity in order to enforce usage policies. For example, local or intermediate networks may wish to implement a limit on simultaneous sessions, and/or may require a billable user identity in order to demonstrate willingness to pay and limit the potential for fraud.

This basically implies that a unique identity known by the home network needs to be conveyed to all parties involved in the roaming transaction for correlating the authentication and accounting packets.

Providing a unique identity to intermediaries is therefore a requirement to fulfill certain business needs. This fulfillment need not undermine the need to protect the anonymity of the user. The mechanism provided by this draft allows the home operator to meet these business requirements by providing a temporal identity representing the subscriber and at the same time protecting the anonymity of the subscriber.

Standard RADIUS Class(25) or UserName(1) attributes could be used to indicate the unique identity - hereafter it is referred to as the Chargeable User Identity (CUI). However, in a complex global roaming environment where there could be one or more intermediary between the NAS and the home RADIUS server, the use of aforementioned attributes could lead to problems as described below.

- On use of RADIUS Class(25) attribute, [RFC2865] states ôThis Attribute is available to be sent by the server to the client in an Access-Accept and SHOULD be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. The client MUST NOT interpret the attribute locally.ö So RADIUS clients for intermediaries MUST NOT interpret the Class(25) attribute, which precludes determining whether it contains a CUI. Furthermore, there could be multiple class attributes in a RADIUS packet with unspecified ordering, which makes it hard to the entities outside home network to determine which one contains the CUI.

- On use of RADIUS UserName(1), the home network could use UserName(1) in the Access-Accept message to convey the CUI to intermediaries and the NAS. However, as the Access-Accept packet

is routed to the NAS, the UserName(1) attribute could be (completely) rewritten by an intermediary and therefore the NAS or other intermediaries along the way will not have access to the CUI. Furthermore, the NAS may use the original value of the UserName(1) attribute (the one sent in the Access-Request packet) in the Accounting-Request packets to ensure the billing follows the same path as authentication packets.

The CUI attribute provides a solution to the above problem and avoids overloading the use of current RADIUS attributes (e.g., UserName(1) re-write). When the home network assigns a value to the CUI it asserts that this value represents a user in the home network. The assertion should be temporary. Long enough to be useful for the external applications and not too long to such that it can be used to identify the user.

1.1 Terminology

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. Operation

This document assumes that the RADIUS protocol operates as specified in [RFC2865], [RFC2866], and the Diameter protocol as specified in [RFC3588].

2.1 Chargeable User Identity Attribute (CUI)

This attribute serves as an alias to the userÆs identity. It is assigned by the home RADIUS server and MAY be sent in Access-Accept message. The NAS or the access network AAA server MUST include this attribute in the Accounting Requests (Start, Interim, and Stop) messages if it was included in the Access Accept message and supported by the NAS. Entities (e.g., NASes, proxies) outside the home network MUST NOT modify the CUI attribute.

The NAS SHOULD include the CUI attribute with a nul character for its data field in the Access-Request message to indicate its support for this attribute to the home RADIUS server. In cases where the CUI is required for proper billing and the home RADIUS server cannot

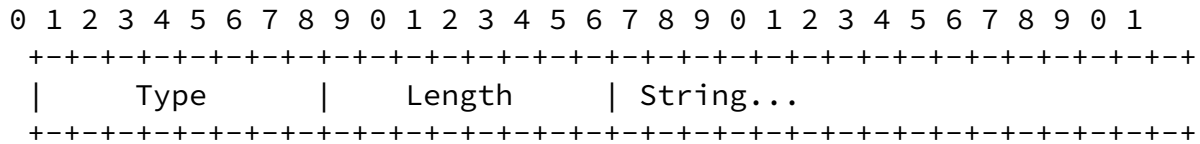
determine the NAS support for the CUI, the home RADIUS server MUST

reject the request by sending an Access-Reject message containing a Reply-Message(18) attribute indicating the failure text: "Support for CUI is required. [Author's notes: indicating the text error message via Reply-Message may not be useful to the NAS - we may want to use the error codes specifed in draft-zorn-radius-err-msg-01.txt.]

if the CUI attribute is not included in the Access-Accept after the CUI support was indicated to the home RADIUS server in the Access-Request, the NAS MAY treat the Access-Accept as an Access-Reject. [Author's notes: I am sure there will be some reaction to this statement, so let's discuss!]

If the RADIUS server includes this attribute in an Access-Accept message it MAY also use this attribute as one of the identity attributes in a Disconnect Message and Change of Authorization message defined by [RFC3576].

A summary of the RADIUS CUI Attribute is given below.



Type: TBD for Chargeable User Identity.

Length: >= 3

String:

The string identifies the CUI of the end-user and is of type UTF8String. It consists of two colon separated parts. The first part determines the CUI type and the second part is the actual Chargeable User Identity value. The CUI type is coded as two octet string representing a hexadecimal number. The CUI value must be at least one octet. In cases where the attribute is used to indicate the NAS support for the CUI, the string value contain a nul character.
The following User-Identity types have been defined:

00 ¡ E.164 number
The identifier is in international E.164 format (e.g. MSISDN, according to the ITU-T E.164 numbering plan as defined in [E164] and [CE164]).

01 ¡ IMSI
The is in international IMSI format according to the ITU-T E.212 numbering plan as defined in [E212] and [CE212]).

02 ¡ SIP URI
The identifier is in the form of a SIP URI as defined (as defined in [RFC3261]).

03 ¡ NAI
The identifier is in the form of a Network Access Identifier as defined in [rfc2486bis].

04 ¡ Opaque string
Opaque string is a value that is assigned to the user by the home network in an unspecified format. where the home network asserts that this value represents a particular user ¡ itÆs a

handle to the user.

05 ¡ reserved

The length of time for which the CUI is valid is unspecified by this specification and typically would be long enough to serve some business needs and short enough such that it minimizes the chance of revealing the true identity of the user (either directly or indirectly).

Below are examples of CUI strings with NAI and E.164 Charging Types:

ö02:charging-id@realm.orgö
ö03:+4689761234ö
ö05:charging-idö

Ideally, the real user identity should not be revealed through this attribute. However, the operators will have the final word on the used charging type and its identifier.

The following table provides a guide to which attribute(s) may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0	0-1	0	0	0-1	TBD	Chargeable User ID

[Note 1] If the Access-Accept contains CUI then the NAS MUST include the CUI in Accounting Requests (Start, Interim and Stop) packets.

Change of Authorization and Disconnect-Request				
Request	ACK	NAK	#	Attribute
0-1	0	0	TBD	Chargeable User

[Note 2] Where CUI attribute is included in Disconnect-Request or CoA-Request messages, it is used for session identification purposes only. This attribute MUST NOT be used for purposes other than identification (e.g. within CoA-Request messages to request authorization changes).

3. Diameter RADIUS Interoperability

In deployments where both RADIUS clients talking with Diameter Servers or Diameter Client talking with RADIUS server then a translation agent will be deployed and operate in accordance to the NASREQ specification. A counterpart Diameter AVP with a similar content to CUI is Diameter Credit-Control ApplicationÆs Subscription-ID AVP [DiameterCC].

4. IANA Considerations

This document requires the assignment of a new RADIUS attribute number for the CUI attribute.

5. Security considerations

The CUI attribute must be protected against Man-in-the-Middle attacks. The CUI appears in Access-Accept and Accounting Requests packets and is protected by the mechanisms that are defined for RADIUS [RFC2865] and [RFC2866]. Therefore there are no additional security considerations beyond those already identified in [RFC2865] and [RFC2866].

Message-Authenticator(80) and Event-Timestamp can be used to further protect against Man-in-the-middle attacks.

In this document we require that entities outside the home network not modify the value of this attribute yet there are no provisions for protecting against or detecting that a RADIUS Proxy has modified the attribute.

6. Acknowledgements

The authors would like to thank Jari Arkko (of Ericsson), Bernard Aboba (of Microsoft), Blair Bullock (of iPass), Sami Ala-luukko (of Teliasonera), Eugene Chang (of Funk), Mark Grayson (of Cisco), David Mariblanca (of Ericsson), and Greg Weber (of Cisco) for their feedback and guidance.

7. References

7.1 Normative references

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

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[rfc2486bis] Aboba, B., Beadles, M., Arkko, J. and P. Eronen, "The Network Access Identifier", draft-arkko-roamops-rfc2486bis-02 (work in progress), July 2004.

[E164] "The International Public Telecommunication Numbering Plan", , May 1997.

[CE164] "List of ITU-T Recommendation E.164 assigned country codes", , June 2000.

[E212] "The international identification plan for mobile terminals and mobile users", , November 1998.

[CE212] "List of mobile country or geographical area codes", , February 1999.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

7.2 Informative references

[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.

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

[DiameterCC] Hakala, H., Koskinen, j., Stura, M. and J. Loughney, "The Network Access Identifier",

draft-ietf-aaa-diameter-cc-06.txt (work in progress), July 2004.

Authors' Addresses

Farid Adrangi
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97124
USA

Phone: +1 503-712-1791
EMail: farid.adrangi@intel.com

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
Canada

Phone: +1 613-591-9104
EMail: avi@bridgewatersystems.com

Jouni Korhonen
Teliasonera Corporation
P.O.Box 970
FIN-00051,   Sonera
Finland

Phone: +3 58405344455
EMail: jouni.korhonen@teliasonera.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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