Network Working Group
Internet-Draft
Expires: June 9, 2005

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

December 9, 2004

Chargeable User Identity
draft-ietf-radext-chargeable-user-id-00

Status of this Memo

Copyright Notice

Abstract

This document describes a new RADIUS attribute, Chargeable User Identity. This attribute can be used by a home network to identity a

user for the purpose of roaming transactions that occur outside of the home network.

Table of Contents

1. Introduction

Some authentication methods, including EAP-PEAP, EAP-TTLS, EAP-SIM and EAP-AKA, can hide the true identity of the user from RADIUS servers outside of the user's home network. In these methods, the User-Name(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 user. While this mechanism is good practice in some circumstances, there are problems if local and intermediate networks require a user identity in order to enforce usage policies.

For example, local or intermediate networks may limit the number of simultaneous sessions for specific users; they may require a chargeable user identity in order to demonstrate willingness to pay or otherwise limit the potential for fraud.

This implies that an authenticated and unique identity provided by the home network should be able to be conveyed to all parties involved in the roaming transaction for correlating the authentication and accounting packets.

Providing a unique identity, called the Chargeable User Identity (CUI) to intermediaries, is necessary to fulfill certain business needs. This should not undermine 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.

1.1 Motivation

Several organizations, including WISPr, GSMA, 3GPP, Wi-Fi Alliance, IRAP, have been studying mechanisms to provide roaming services, using RADIUS. A mechanism for providing the current deployments with the capacity to deploy, bill and oversee WPA networks against fraud.

The CUI attribute has been designed to close operational loopholes in RADIUS specifications that have impacted roaming solutions negatively, especially when tunneled protocols with multiple identities, such as PEAP or TTLS, are used. A chargeable identity reflecting the user profile authenticated by the home network is needed in such roaming scenarios.

Existing RADIUS servers that do not understand the CUI attribute SHOULD silently discard the attribute. Use of the CUI is geared to multi-identity EAP authentications which are, for the most part, recent deployments.

Some other mechanisms have been proposed in place of the CUI attribute. These mechanisms are insufficient or cause other problems. It has been suggested that standard RADIUS Class(25) or User-Name(1) attributes could be used to indicate the Chargeable User Identity. However, in a complex global roaming environment where there could be one or more intermediaries 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 "This 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." So RADIUS clients for intermediaries MUST NOT interpret the Class(25) attribute, which precludes determining whether it contains a CUI. Additionally, 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 User-Name(1)

The home network could use User-Name(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 User-Name(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 User-Name(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., User-Name(1) re-write). CUI is the correct standards-based approach to fixing the problems which have arisen with multiple-identity RADIUS authorization and accounting methods. It does not solve all related problems, but does provide networks the ability to bill and oversee WPA networks against fraud. 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.

1.2 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].

3GPP - Third Generation Partnership Program
AAA - Authentication, Authorization and Accounting
CUI - Chargeable User Identity
GSMA - GSM Association
IRAP - International Roaming Access Protocols Program
NAS - Network Access Server
PEAP - Protected Extensible Authentication Protocol
TTLS - Tunneled Transport Layer Security
WISPr - Wireless ISP Roaming
WPA - Wi-Fi Protected Access

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 (CUI) Attribute

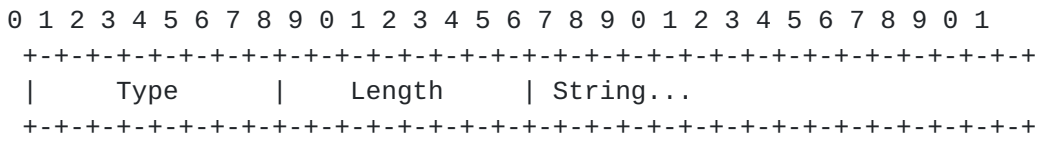
This attribute serves as an alias to the user's identity. It is assigned by the home RADIUS server and MAY be sent in Access-Accept message. The NAS or the access network AAA server MUST include this attribute in the Accounting Requests (Start, Interim, and Stop) messages if it was included in the Access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

The NAS MAY include the CUI attribute with a null 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 home RADIUS server cannot determine the NAS support for the CUI, if the home RADIUS server requires the NAS support for CUI for any reason (e.g., for billing or charging purposes), the home RADIUS server MUST reject the request by sending an Access-Reject message including an Error-Cause attribute [RFC3576] with value (to-be-defined) (decimal), "CUI-Support-Undetermined". Otherwise, if the authentication is successful, the home RADIUS server MUST send both the User-Name (1) attribute and the CUI attribute, with the understanding that if the NAS supports the CUI attribute the CUI attribute will override the identity portion the User-Name (1) attribute. That is, the User-Name(1) attribute will be used for routing and the CUI attribute

will be used for identity purposes.

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 two parts separated by a colon, ':'. 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 strings 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 contains a null 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 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.

05 - reserved

The length of time for which the CUI is valid is outside of the scope of this specification. It is assumed to be deployment related. It should typically 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:

"03:charging-id@realm.org"
"00:+4689761234"
"04:charging-id"

The real user identity SHOULD NOT be revealed through this attribute. However, the value of this attribute is determined by the service provider.

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
0-1	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 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 with both RADIUS and Diameter interworking, a translation agent will be deployed and operate in accordance to the NASREQ specification. The Diameter Credit-Control Application's specifies a similar concept, the Subscription-ID AVP [DiameterCC].

4. IANA Considerations

This document instructs IANA to assign 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, entities outside the home network are required not to modify the value of this attribute, however there are no provisions for protecting against or detecting that a RADIUS Proxy has modified the attribute.

As the CUI contains an identity that can be used for authorizing and accounting of services, this attribute must be protected against snooping.

6. Acknowledgements

The authors would like to thank Jari Arkko, Bernard Aboba, David Nelson, Blair Bullock, Sami Ala-Luukko, Lothar Reith, David Mariblanca, Eugene Chang, Greg Weber, and Mark Grayson, 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: +358405344455
EMail: jouni.korhonen@teliasonera.com

John Loughney
Nokia
Itamerenkatu 11-13
FIN-00180, Helsinki
Finland

Phone: +358504836342
EMail: john.loughney@nokia.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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