Network Working Group
Internet-Draft
Expires: September 23, 2005

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

March 22, 2005

Chargeable User Identity
draft-ietf-radext-chargeable-user-id-04

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of Section 3 of RFC 3667. By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 23, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document describes a new RADIUS attribute,

Chargeable-User-Identity. This attribute can be used by a home network to identify a user for the purpose of roaming transactions that occur outside of the home network.

Table of Contents

1. Introduction 3
1.1 Motivation 4
1.2 Terminology 5
2. Operation 5
2.1 Chargeable-User-Identity (CUI) Attribute 5
2.2 CUI Attribute 6
3. Attribute Table 7
4. Diameter Consideration 7
5. IANA Considerations 7
6. Security considerations 7
7. Acknowledgements 8
8. References 8
8.1 Normative references 8
8.2 Informative references 8
Authors' Addresses 9
Intellectual Property and Copyright Statements 10

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 surrogate identity to bind the current session.

This document introduces an attribute that serves as an alias or handle (hereafter, it is called Chargeable-User-Identity) to the real user's identity. Chargeable-User-Identity can be used outside the home network in scenarios that traditionaly relied on User-Name(1) to correlate a session to a user.

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 a 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, 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 temporary identity representing the subscriber and at the same time protecting the anonymity of the subscriber.

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 such that it can be used to identify the user.

Several organizations, including WISPr, GSMA, 3GPP, Wi-Fi Alliance, IRAP, have been studying mechanisms to provide roaming services, using RADIUS. Missing elements include mechanisms for billing and fraud prevention.

The CUI attribute is intended to close operational loopholes in

RADIUS specifications that have impacted roaming solutions negatively. Use of the CUI is geared toward EAP methods supporting privacy (such as PEAP and EAP-TTLS), which are, for the most part, recent deployments. A chargeable identity reflecting the user profile by the home network is needed in such roaming scenarios.

1.1 Motivation

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 CUI. 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 the 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 packet 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 or 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, and since the contents of Class(25) attribute is not to be interpreted by clients, this makes it hard to the entities outside home network to determine which one contains the CUI.

- On the use of RADIUS User-Name(1) attribute:

The User-Name(1) attribute included in the Access-Request packet may be used for the purpose of routing the Access-Request packet, and in the process may be rewritten by intermediaries. As a result, a RADIUS server receiving an Access-Request packet relayed by a proxy cannot assume that the User-Name(1) attribute remained unmodified.
On the other hand, rewriting of a User-Name(1) attribute sent within an Access-Accept packet occurs more rarely, since a Proxy-State(33) attribute can be used to route the Access-Accept packet without parsing the User-Name(1) attribute. As a result, a RADIUS server cannot assume that a proxy stripping routing information from a User-Name(1) attribute within an Access-Request packet will add this information to a User-Name(1) attribute included within an Access-Accept packet. The result is that when a User-Name(1) attribute is sent in an Access-Accept packet it is

possible that the Access-Request packet and Accounting-Request packets will follow different paths. Where this outcome is undesirable, the RADIUS client should use the original User-Name(1) in accounting packets. Therfore, another mechanism is required to convey a CUI within an Access-Accept packet to the RADIUS client, so that the CUI can be included in the accounting packets.

The CUI attribute provides a solution to the above problems and avoids overloading RADIUS User-Name(1) attribute or changing the usage of existing RADIUS Class(25) attribute. The CUI therefore provides a standard approach to billing and fraud prevention when EAP methods supporting privacy are used. It does not solve all related problems, but does provide for billing and fraud prevention.

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], dynamic authorization as specified in [RFC3576], and the Diameter protocol as specified in [RFC3588].

2.1 Chargeable-User-Identity (CUI) Attribute

The CUI attribute serves as an alias to the user's real identity, representing a chargeable identity as defined and provided by the home network as a supplemental or alternative information to User-Name(1). Typically the CUI represents the identity of the actual user but it may also indicate other chargeable identities such as a group of users. RADIUS clients (proxy or NAS) outside the home network MUST NOT modify the CUI attribute.

The RADIUS server (a RADIUS proxy, home RADIUS server) may include the CUI attribute in the Access-Accept packet destined to a roaming partner. The CUI support by RADIUS infrastructure is driven by the business requirements between roaming entities. Therefore a RADIUS server supporting this specification may not choose to send the CUI in response to an Access-Request packet from a given NAS, even if the NAS has indicated that it supports CUI.

If an Access-Accept packet without the CUI attribute was received by a RADIUS client that requested the CUI attribute, then the Access-Accept packet MAY be treated as an Access-Reject.

If the CUI was included in an Access-Accept packet, RADIUS clients supporting the CUI attribute MUST ensure that the CUI attribute appears in the RADIUS Accounting-Request (Start, Interim, and Stop).

RFC 2865 includes the following statements about behaviors of RADIUS client and server with respect to unsupported attributes:

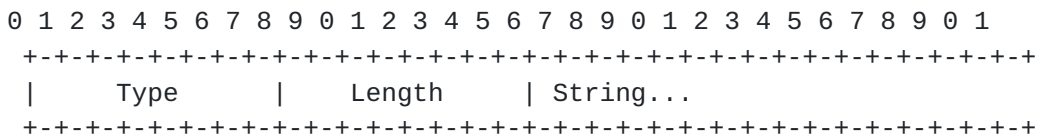
- "A RADIUS client MAY ignore Attributes with an unknown Type."
- "A RADIUS server MAY ignore Attributes with an unknown Type."

Therefore, RADIUS clients or servers that do not support the CUI may ignore the attribute. A RADIUS client requesting the CUI attribute in an Access-Accept packet MUST include within the Access-Request packet a CUI attribute with a single NUL character (referred to as a nul CUI).

If a home RADIUS server that supports the CUI attribute receives an Access-Request packet containing a CUI (set to nul or otherwise), it MUST include the CUI attribute in the Access-Accept packet. Otherwise, if the Access-Request packet does not contain a CUI, the home RADIUS server MUST NOT include the CUI attribute in the Access-Accept packet.

2.2 CUI Attribute

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. This string value is a reference to a particular user. The format and content of the string value is determined by the Home RADIUS server. The binding lifetime of the reference to the user is determined based on business agreements. For example, the lifetime can be set to one billing period. RADIUS entities other than the Home RADIUS server MUST treat the CUI content as an opaque token, and SHOULD NOT perform operations on its content other than a binary equality comparison test, between two instances of CUI. In cases where the attribute is used to indicate the NAS support for the CUI, the string value contains a nul character.

3. Attribute Table

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-identity

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

4. Diameter Consideration

Diameter needs to define an identical attribute with the same Type value. The CUI should be available as part of the NASREQ application.

5. IANA Considerations

This document uses the RADIUS [RFC2865] namespace, see "http://www.iana.org/assignments/radius-types". This document instructs IANA to assign a new RADIUS attribute number for the CUI attribute.

CUI TBA

6. Security considerations

It is strongly recommended that the CUI format used is such that the real user identity is not revealed. Furthermore, where a reference

is used to a real user identity, the binding lifetime of that reference to the real user be kept as short as possible.

The RADIUS entities (RADIUS proxies and clients)outside the home netowrk MUST NOT modify the CUI. However, there is no way to detect or prevent this.

If the NAS includes CUI in an Access-Request packet, a man-in-the-middle may remove it. This will cause the Access-Accept packet to not include a CUI attribute, which may cause the NAS to reject the session. To prevent such a DoS attack, the NAS SHOULD include a Message-Authenticator(80) attribute within Access-Request packets containing a CUI attribute.

7. Acknowledgements

The authors would like to thank Jari Arkko, Bernard Aboba, David Nelson, Barney Wolff, Blair Bullock, Sami Ala-Luukko, Lothar Reith, David Mariblanca, Eugene Chang, Greg Weber, and Mark Grayson, for their feedback and guidance.

8. References

8.1 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", Internet-Draft draft-arkko-roamops-rfc2486bis-02, July 2004.

8.2 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.

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

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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