Groupe de travail Réseau
Request for Comments : 4372
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

F. Adrangi, Intel
A. Lior, Bridgewater Systems
J. Korhonen, Teliasonera
J. Loughney, Nokia
janvier 2006

Identité d'utilisateur facturable

Résumé
Le présent document décrit un nouvel attribut du service d'authentification à distance de l'utilisateur appelant (RADIUS, *Remote Authentication Dial-In User Service*) identité de l'utilisateur facturable *(Chargeable-User-Identity)*. Cet attribut peut être utilisé par un réseau de rattachement pour identifier un utilisateur pour les besoins de transactions d'itinérance qui se produisent en dehors du réseau de rattachement.

Table des matières

1. Introduction

Certaines méthodes d'authentification, incluant EAP-PEAP, EAP-TTLS, EAP-SIM et EAP-AKA, peuvent cacher la véritable identité de l'utilisateur aux serveurs RADIUS en dehors du réseau de rattachement de l'utilisateur. Dans ces méthodes, l'attribut Nom-d'utilisateur(1) *(User-Name)* contient une identité anonyme (par exemple, @exemple.com) suffisante pour acheminer les paquets RADIUS au réseau de rattachement mais par ailleurs insuffisante pour identifier l'utilisateur. Bien que ce mécanisme soit de bonne pratique dans certaines circonstances, il y a des problèmes si les réseaux locaux et intermédiaires exigent une identité de substitution pour lier la session en cours.

Le présent document introduit un attribut qui sert d'alias ou de bride (qu'on appelle ici l'identité d'utilisateur facturable) à l'identité réelle de l'utilisateur. L'identité d'utilisateur facturable peut être utilisée en dehors du réseau de rattachement dans des scénarios qui s'appuient traditionnellement sur Nom-d'utilisateur(1) pour corréler une session à un utilisateur.

Par exemple, les réseaux locaux ou intermédiaires peuvent limiter le nombre de sessions simultanées pour des utilisateurs spécifiques ; ils peuvent exiger une identité d'utilisateur facturable afin de démontrer leur volonté de payer ou limiter par

ailleurs le potentiel de fraude.

Cela implique qu'une identité unique fournie par le réseau de rattachement devrait être capable d'être portée à toutes les parties impliquées dans la transaction d'itinérance pour corréler l'authentification et les paquets de comptabilité.

Fournir une identité unique, l'identité d'utilisateur facturable (CUI, *Chargeable-User-Identity*) aux intermédiaires, est nécessaire pour satisfaire certains besoins commerciaux. Cela ne devrait pas nuire à l'anonymat de l'utilisateur. Le mécanisme fourni par le présent document permet à l'opérateur de rattachement de satisfaire les exigences commerciales en fournissant une identité temporaire qui représente l'utilisateur et en même temps protège l'anonymat de l'utilisateur.

Quand le réseau de rattachement alloue une valeur à la CUI, il affirme que cette valeur représente un usager dans le réseau de rattachement. L'assertion devrait être temporaire – assez longtemps pour être utile pour les applications externes et pas assez longtemps pour qu'elle puisse être utilisée pour identifier l'utilisateur.

Plusieurs organisations, parmi lesquelles WISPr, GSMA, 3GPP, Wi-Fi Alliance, et IRAP, ont étudié ces mécanismes pour fournir des services d'itinérance, en utilisant RADIUS. Les éléments manquants incluent des mécanismes pour la facturation et la prévention de la fraude.

L'attribut CUI est destiné à boucher les trous de fonctionnement des spécifications de RADIUS qui ont eu un impact négatif sur les solutions d'itinérance. L'utilisation de la CUI est articulée sur les méthodes EAP qui prennent en charge la confidentialité (comme PEAP et EAP-TTLS) qui sont pour la plupart, des déploiements récents. Une identité de facturation reflétant le profil de l'utilisateur par le réseau de rattachement est nécessaire dans de tels scénarios d'itinérance.

1.1 Motifs

Quelques autres mécanismes ont été proposés à la place de l'attribut CUI. Ces mécanismes sont insuffisants ou causent d'autres problèmes. Il a été suggéré que les attributs standard RADIUS Class(25) ou Nom-d'utilisateur(1) pourraient être utilisés pour indiquer la CUI. Cependant, dans un environnement d'itinérance globale complexe où il pourrait y avoir un ou plusieurs intermédiaires entre le serveur d'accès réseau (NAS, *Network Access Server*) [RFC4282] et le serveur RADIUS de rattachement, l'utilisation des attributs susmentionnés pourrait conduire aux problèmes décrits ci-dessous :

- Sur l'utilisation de l'attribut RADIUS Class(25) :
La [RFC2865] déclare : "Cet attribut est disponible pour être envoyé par le serveur au client dans un paquet Accés-Accepté et DEVRAIT être envoyé non modifié par le client au serveur de comptabilité au titre du paquet Demande-de-comptabilité si la comptabilité est prise en charge. Le client NE DOIT PAS interpréter l'attribut localement." Ainsi, les clients RADIUS ou les intermédiaires NE DOIVENT PAS interpréter l'attribut Class(25), ce qui empêche de déterminer si il contient une CUI. De plus, il peut y avoir plusieurs attributs de classe dans un paquet RADIUS, et comme le contenu de l'attribut Class(25) ne peut pas être interprété par les clients, cela rend difficile aux entités en dehors du réseau de rattachement de déterminer quels sont ceux qui contiennent la CUI.

- Sur l'utilisation de l'attribut RADIUS Nom-d'utilisateur(1) :
L'attribut Nom-d'utilisateur(1) inclus dans le paquet Demande-d'accès peut être utilisé pour les besoins de l'acheminement du paquet Demande-d'accès, et dans ce processus peut être reécrit par des intermédiaires. Par suite, un serveur RADIUS qui reçoit un paquet Demande-d'accès relayé par un mandataire ne peut pas supposer que l'attribut Nom-d'utilisateur(1) n'a pas été modifié.

Par ailleurs, la reécriture d'un attribut Nom-d'utilisateur(1) envoyé au sein d'un paquet Accès-Accepté survient plus rarement, car un attribut État-de-mandataire(33) peut être utilisé pour acheminer le paquet Accès-Accepté sans analyser l'attribut Nom-d'utilisateur(1). Par suite, un serveur RADIUS ne peut pas supposer qu'un mandataire qui efface des informations d'acheminement d'un attribut Nom-d'utilisateur(1) au sein d'un paquet Demande-d'accès va ajouter ces informations à un attribut Nom-d'utilisateur(1) inclus dans un paquet Accès-Accepté. Le résultat est que quand un attribut Nom-d'utilisateur(1) est envoyé dans un paquet Accès-Accepté, il est possible que le paquet Demande-d'accès et les paquets Demande-de-comptabilité suivent des chemins différents. Lorsque ce résultat est indésirable, le client RADIUS devrait utiliser le Nom-d'utilisateur(1) original dans les paquets de comptabilité. Donc, un autre mécanisme est nécessaire pour porter une CUI au sein d'un paquet Accès-Accepté au client RADIUS, afin que la CUI puisse être incluse dans les paquets de comptabilité.

L'attribut CUI fournit une solution aux problèmes ci-dessus et évite de surcharger l'attribut RADIUS Nom-d'utilisateur(1) ou de changer l'usage de l'attribut existant RADIUS Class(25). La CUI fournit donc une approche standard pour la facturation et la prévention de la fraude quand les méthodes EAP qui prennent en charge la confidentialité sont utilisées.

Elle ne résoud pas tous les problèmes, mais assure la facturation et la prévention de la fraude.

1.2 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Les acronymes suivants sont utilisés :

3GPP *(Third Generation Partnership Project)* projet en partenariat de troisième génération
AAA *(Authentication, Authorization, and Accounting)* authentification, autorisation, et comptabilité
AKA *(Authentication and Key Agreement)* authentification et accord de clé
CUI *(Chargeable-User-Identity)* identité d'utilisateur facturable
GSMA *(GSM Association)* association GSM
IRAP *(International Roaming Access Protocols Program)* programme de protocoles d'accès à l'itinérance internationale
NAS *(Network Access Server)* serveur d'accès réseau
PEAP *(Protected Extensible Authentication Protocol)* protocole d'authentification extensible protégée
SIM *(Subscriber Identity Module)* module d'identité d'abonné
TTLS *(Tunneled Transport Layer Security)* sécurité de la couche transport tunnelée
WISPr *(Wireless ISP Roaming)* itinérance de fournisseur d'accès sans fil
WPA *(Wi-Fi Protected Access)* accès Wi-Fi protégé

2. Fonctionnement

Le présent document suppose que le protocole RADIUS opère comme spécifié dans les [RFC2865] et [RFC2866], avec l'autorisation dynamique spécifiée dans la [RFC3576], et le protocole Diameter spécifié dans la [RFC3588].

2.1 Attribut Identité d'utilisateur facturable (CUI)

L'attribut CUI sert d'alias à l'identité réelle de l'utilisateur, représentant une identité facturable comme défini et assuré par le réseau de rattachement comme information supplémentaire ou de remplacement au Nom-d'utilisateur(1). Normalement, la CUI représente l'identité de l'utilisateur réel, mais elle peut aussi indiquer d'autres identités facturables comme un groupe d'utilisateurs. Les clients RADIUS (mandataires ou NAS) hors du réseau de rattachement NE DOIVENT PAS modifier l'attribut CUI.

Le serveur RADIUS (un mandataire RADIUS, le serveur RADIUS de rattachement) peut inclure l'attribut CUI dans le paquet Accès-Accepté destiné à un partenaire d'itinérance. La prise en charge de la CUI par l'infrastructure RADIUS est conduite par les exigences d'affaires entre les entités d'itinérance. Donc, un serveur RADIUS qui prend en charge la présente spécification peut choisir de ne pas envoyer la CUI en réponse à un paquet Demande-d'accès provenant d'un certain NAS, même si le NAS a indiqué qu'il prend en charge la CUI.

Si un paquet Accès-Accepté sans l'attribut CUI a été reçu par un client RADIUS qui demandait l'attribut CUI, le paquet Accès-Accepté PEUT alors être traité comme un Accès-rejeté.

Si la CUI a été incluse dans un paquet Accès-Accepté, les clients RADIUS qui prennent en charge l'attribut CUI DOIVENT s'assurer que l'attribut CUI apparaît dans la Demande-de-comptabilité RADIUS (Start, Interim, et Stop). Cette exigence s'applique sans considération de si le client RADIUS a demandé l'attribut CUI.

La RFC 2865 inclut les déclarations suivantes sur les comportements de client et serveur RADIUS à l'égard des attributs non pris en charge :
- "Un client RADIUS PEUT ignorer les attributs d'un type inconnu."
- "Un serveur RADIUS PEUT ignorer les attributs d'un type inconnu."

Donc, les clients et serveurs RADIUS qui ne prennent pas en charge la CUI peuvent ignorer l'attribut.

Un client RADIUS qui demande l'attribut CUI dans un paquet Accès-Accepté DOIT inclure dans le paquet Demande-d'accès un attribut CUI. Pour l'authentification initiale, l'attribut CUI va inclure un seul caractère NUL (appelé une CUI

nulle). Et, durant la réauthentification, l'attribut CUI va inclure la valeur de CUI précédemment reçue (appelée une valeur de CUI non nulle) dans le Accès-Accepté.

À réception d'une valeur de CUI non nulle dans une Demande-d'accès, le serveur de rattachement RADIUS PEUT vérifier que la valeur de la CUI correspond à la CUI provenant du précédent Accès-Accepté. Si la vérification échoue, le serveur RADIUS DEVRAIT alors répondre par un message Accès-rejeté.

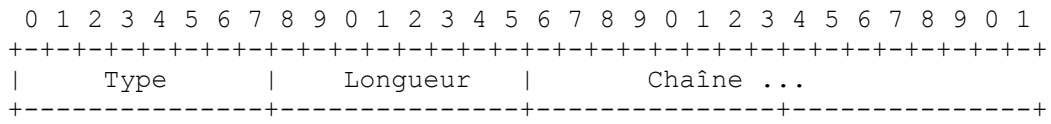
Si un serveur de rattachement RADIUS qui prend en charge l'attribut CUI reçoit un paquet Demande-d'accès contenant une CUI (réglée à NUL ou autrement) il DOIT inclure l'attribut CUI dans le paquet Accès-Accepté.

Autrement, si le paquet Demande-d'accès ne contient pas de CUI, le serveur de rattachement RADIUS NE DEVRAIT PAS inclure l'attribut CUI dans le paquet Accès-Accepté. La demande d'accès peut être envoyée dans l'authentification initiale ou durant la réauthentification.

Un NAS qui a demandé la CUI durant la réauthentification en incluant la CUI dans la demande d'accès va recevoir la CUI dans le Accès-Accepté. Le NAS DOIT inclure la valeur de cette CUI dans tous les messages de comptabilité.

2.2 Attribut CUI

Le format de l'attribut RADIUS CUI est donné ci-dessous :



Type : 89 pour Identité d'utilisateur facturable.

Longueur : ≥ 3

Chaîne : La chaîne identifie la CUI de l'utilisateur final. Cette valeur de chaîne est une référence à un utilisateur particulier. Le format et le contenu de la valeur de la chaîne sont déterminés par le serveur de rattachement RADIUS. La durée de vie du lien de la référence à l'utilisateur est déterminée sur la base des accords d'affaires. Par exemple, la durée de vie peut être réglée à une période de facturation. Les entités RADIUS autres que les serveurs de rattachement RADIUS DOIVENT traiter le contenu de la CUI comme un jeton opaque, et NE DEVRAIENT PAS effectuer d'opérations sur son contenu autre qu'une vérification de comparaison d'égalité binaire entre deux instances de CUI. Dans les cas où l'attribut est utilisé pour indiquer la prise en charge de la CUI par le NAS, la valeur de la chaîne contient un caractère nul.

3. Tableau d'attributs

Le tableau suivant indique quels attributs peuvent être trouvés dans les différents types de paquets, et en quelle quantité.

Demande	Accepté	Rejeté	Défi	Demande-de-comptabilité	n°	Attribut
0-1	0-1	0	0	0-1	89	Identité d'utilisateur facturable

Légende :
0 Cet attribut NE DOIT PAS être présent dans le paquet.
0-1 Zéro ou une instance de cet attribut PEUT être présente dans le paquet
1 Exactement une instance de cet attribut DOIT être présente dans le paquet.

Note : Si le paquet Accès-Accepté contient une CUI, le NAS DOIT alors inclure la CUI dans les paquets Demande-de-comptabilité (Start, Interim, et Stop).

6. Considérations relatives à Diameter

Diameter doit définir un attribut identique avec la même valeur de Type. La CUI devrait être disponible au titre de l'application NASREQ [RFC4005].

5. Considérations relatives à l'IANA

Le présent document utilise l'espace de noms RADIUS [RFC2865] ; voir à http://www.iana.org/assignments/radius-types. L'IANA a alloué un nouveau numéro d'attribut RADIUS pour l'attribut CUI : CUI 89

6. Considérations sur la sécurité

Il est fortement recommandé que le format de CUI utilisé soit tel que l'identité de l'utilisateur réel ne soit pas révélée. De plus, lorsque est utilisée une référence à une identité réelle d'utilisateur, il est recommandé que la durée de vie du lien de cette référence reste aussi courte que possible.

Les entités RADIUS (mandataires et clients RADIUS) en dehors du réseau de rattachement NE DOIVENT PAS modifier la CUI ou insérer une CUI dans un Accès-Accepté. Cependant, il n'y a pas de moyen de le détecter ou l'empêcher.

Pour tenter un vol de service, un interposé peut essayer d'insérer, modifier, ou supprimer la CUI dans les paquets Accès-Accepté et les paquets de comptabilité. Cependant, les paquets RADIUS Accès-Accepté et Comptabilité fournissent déjà la protection de l'intégrité.

Si le NAS inclut la CUI dans un paquet Demande-d'accès, un interposé peut la retirer. Cela va causer la non inclusion de l'attribut CUI dans le paquet Accès-Accepté, ce qui peut causer le rejet de la session par le NAS. Pour empêcher une telle attaque de déni de service, le NAS DEVRAIT inclure un attribut Authentifiant-de-message(80) dans les paquets Demande-d'accès qui contiennent un attribut CUI.

7. Remerciements

Les auteurs tiennent à remercier Jari Arkko, Bernard Aboba, David Nelson, Barney Wolff, Blair Bullock, Sami Ala-Luukko, Lothar Reith, David Mariblanca, Eugene Chang, Greg Weber, et Mark Grayson de leurs retours et conseils.

8. Références normatives

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. *(D.S.)* (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044)

[RFC2866] C. Rigney, "Comptabilité RADIUS", juin 2000. *(Information)* (*MàJ par* RFC2867, RFC5080)

[RFC4005] P. Calhoun et autres, "Application de serveur d'accès réseau Diameter", août 2005. *(P.S.) (Remplacée par* RFC7155)

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. *(P.S., Remplacée par* RFC7542)

8.2 Références pour information

[RFC3576] M. Chiba et autres, "Extensions d'autorisation dynamique au service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. *(Information)* (*Obsolète, voir* RFC5176)

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. *(P.S.)* (*Remplacée par la* RFC6733)

Adresse des auteurs

Farid Adrangi
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97124
USA
téléphone : +1 503-712-1791
mél : farid.adrangi@intel.com

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
Canada
téléphone : +1 613-591-9104
mél : avi@bridgewatersystems.com

Jouni Korhonen
Teliasonera Corporation
P.O.Box 970
FIN-00051, Sonera
Finland
téléphone : +358405344455
mél : jouni.korhonen@teliasonera.com

John Loughney
Nokia
Itamerenkatu 11-13
FIN-00180, Helsinki
Finland
téléphone : +358504836342
mél : john.loughney@nokia.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.