Groupe de travail Réseau
Request for Comments : 4505
RFC rendue obsolète : 2245
Catégorie : Sur la voie de la normalisation

K. Zeilenga, éd. OpenLDAP Foundation

juin 2006
Traduction Claude Brière de L'Isle

Mécanisme anonyme pour authentification simple et couche de sécurité (SASL)

Résumé
Sur l'Internet, il est de pratique courante de permettre un accès anonyme à divers services. Traditionnellement, ceci a été fait avec un mécanisme de mot de passe en clair utilisant "anonymous" comme nom d'utilisateur et en utilisant des informations facultatives de trace, comme une adresse de messagerie électronique, comme mot de passe. Comme les commandes de connexion en texte en clair ne sont plus permises dans les nouveaux protocoles de l'IETF, une nouvelle façon de fournir une connexion anonyme est nécessaire dans le contexte du cadre d'authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*).

1. Introduction

Le présent document définit un mécanisme anonyme pour le cadre d'authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*) [RFC4422]. Le nom associé à ce mécanisme est "ANONYMOUS".

À la différence des autres mécanismes SASL, dont l'objet est d'authentifier et identifier l'utilisateur auprès d'un serveur, l'objet de ce mécanisme SASL est de permettre à l'utilisateur d'obtenir l'accès à des services ou ressources sans exiger que l'utilisateur établisse ou divulgue autrement son identité au serveur. C'est -à-dire que ce mécanisme fournit une méthode de connexion anonyme.

Ce mécanisme ne fournit pas de couche de sécurité.

Le présent document remplace la RFC 2245. Les changements par rapport à la RFC 2245 sont détaillés à l'Appendice A.

2. Mécanisme anonyme

Le mécanisme consiste en un seul message du client au serveur. Le client peut inclure dans ce message des informations de trace sous la forme d'une chaîne de caractères [Unicode] codés selon la [RFC3629] préparée en accord avec la [RFC3454] et le profil "trace" stringprep défini à la Section 3 du présent document. Les informations de trace, qui n'ont pas de valeur sémantique, devraient prendre une des deux formes suivantes : une adresse de messagerie électronique Internet, ou une chaîne opaque qui ne contient pas le caractère '@' (U+0040) et qui peut être interprétée par l'administrateur de système du domaine du client. Pour des raisons de confidentialité, une adresse de messagerie électronique Internet ou d'autres informations identifiant l'utilisateur ne devraient être utilisées qu'avec la permission de l'utilisateur.

Un serveur qui permet un accès anonyme va annoncer la prise en charge du mécanisme ANONYMOUS et permettre à tous de se connecter en utilisant ce mécanisme, généralement avec un accès restreint.

On fournit ci dessous une grammaire formelle pour le message du client qui utilise le BNF augmenté [RFC4234] comme outil pour comprendre cette spécification technique.

```
message = [ email / token ]                ;; à préparer en accord avec la Section 3

UTF1 = %x00-3F / %x41-7F                   ;; moins '@' (U+0040)
UTF2 = %xC2-DF UTF0
UTF3 = %xE0 %xA0-BF UTF0 / %xE1-EC 2(UTF0) / %xED %x80-9F UTF0 / %xEE-EF 2(UTF0)
UTF4 = %xF0 %x90-BF 2(UTF0) / %xF1-F3 3(UTF0) / %xF4 %x80-8F 2(UTF0)
UTF0 = %x80-BF

TCHAR = UTF1 / UTF2 / UTF3 / UTF4
;; tout caractère Unicode codé en UTF-8 sauf le caractère '@' (U+0040)

email  = addr-spec                         ;; comme défini dans la [[RFC2822]

token  = 1*255TCHAR
```

Note de mise en œuvre : la production <token> *(jeton)* est restreinte aux 255 caractères Unicode codés en UTF-8. Comme le codage des caractères utilise une séquence de 1 à 4 octets, un jeton peut faire jusqu'à 1020 octets.

3. Profil "trace" de "Stringprep"

Cette Section définit le profil "trace" de la [RFC3454]. Ce profil est conçu pour être utilisé avec le mécanisme SASL ANONYMOUS. Précisément, le client doit préparer la production <message> en accord avec ce profil.

Le répertoire de caractères de ce profil est Unicode 3.2 [Unicode].

Aucune transposition n'est requise par ce profil.

Aucune normalisation Unicode n'est requise par ce profil.

La liste des codets non alloués pour ce profil est celle fournie dans l'Appendice A de la [RFC3454]. Les codets non alloués ne sont pas interdits.

Les caractères provenant des tableaux suivants de la [RFC3454] sont interdits :
- C.2.1 (caractères de contrôle ASCII)
- C.2.2 (caractères de contrôle non ASCII)
- C.3 (caractères d'utilisation privée)
- C.4 (codets non de caractères)
- C.5 (codes de substitution)
- C.6 (inappropriés pour le texte pur)
- C.8 (le changement des propriétés d'affichage sont déconseillées)
- C.9 (caractères d'étiquetage)

Aucun caractère supplémentaire n'est interdit.

Ce profil exige la vérification des caractères bidirectionnels conformément à la Section 6 de la [RFC3454].

4. Exemple

Voici un exemple de connexion ANONYMOUS entre un client et un serveur IMAP.
Dans cet exemple, "C:" et "S:" indiquent les lignes envoyées respectivement par le client et le serveur. Si ces lignes commencent sans une nouvelle étiquette "C:" ou "S:" le saut à la ligne est pour la clarté rédactionnelle et ne fait pas partie de la commande.

Noter que cet exemple utilise le profil IMAP [RFC3501] de SASL. Le codage base64 des défis et réponses ainsi que le "+"

précédant les réponses font partie du profil IMAP4, et non de SASL lui-même. De plus, les protocoles avec des profils SASL qui permettent une réponse initiale de client seront capable d'éviter l'aller-retour supplémentaire ci-dessous (la réponse de serveur avec un "+ " vide).

Dans cet exemple, les informations de trace sont "sirhc".

S: * OK serveur IMAP4 prêt
C: A001 CAPABILITY
S: * CAPABILITY IMAP4 IMAP4rev1 AUTH=DIGEST-MD5 AUTH=ANONYMOUS
S: A001 OK fait
C: A002 AUTHENTICATE ANONYMOUS
S: +
C: c2lyaGM=
S: A003 OK Bienvenue, les informations de trace ont été enregistrées.

5. Considérations sur la sécurité

Le mécanisme ANONYMOUS accorde à tous l'accès à des services et/ou ressources. Pour cette raison, il devrait être désactivé par défaut afin que l'administrateur puisse prendre la décision explicite de l'activer.

Si l'utilisateur anonyme a des privilèges d'écriture, une attaque de déni de service est possible en remplissant tout l'espace disponible. Cela peut être empêché en désactivant tous les accès en écriture par les utilisateurs anonymes.

Si des utilisateurs anonymes ont un accès en lecture et écriture à la même zone, le serveur peut être utilisé comme mécanisme de communication pour échanger anonymement des informations. Les serveurs qui acceptent des soumissions anonymes devraient mettre en œuvre le modèle commun de "boîte à ordures" qui interdit l'accès anonyme en lecture à la zone où les soumissions anonymes sont acceptées.

Si l'utilisateur anonyme peut effectuer de nombreuses opérations coûteuses (par exemple, une commande IMAP SEARCH BODY) cela pourrait activer une attaque de déni de service. Les serveurs sont invités à réduire la priorité de utilisateurs anonymes ou à limiter leur utilisation de ressources.

Alors que les serveurs peuvent imposer une limite au nombre d'utilisateurs anonymes, on notera que de telles limites activent des attaques de déni de service et devraient être utilisées avec prudence.

Les informations de trace ne sont pas authentifiées, de sorte qu'elles peuvent être falsifiées. Cela peut être utilisé comme tentative de mettre quelqu'un d'autre dans des difficultés pour accéder à des informations discutables. Les administrateurs qui font des investigations sur des abus doivent réaliser que ces informations de trace peuvent être falsifiées.

Un client qui utilise l'adresse de messagerie électronique correcte de l'usager comme informations de trace sans permission explicite peut violer la confidentialité de cet utilisateur. Quiconque a accès à une archive anonyme sur un sujet sensible (par exemple, des abus sexuels) a probablement un fort besoin de confidentialité. Les clients ne devraient pas envoyer leur adresse de messagerie électronique sans la permission explicite de l'utilisateur et devraient offrir l'option de ne pas fournir d'informations de trace, exposant donc seulement l'adresse IP de source et l'heure.

Les serveurs mandataires anonymes pourraient améliorer cette confidentialité mais devraient considérer les attaques de déni de service potentielles résultantes.

Les connexions anonymes sont susceptibles d’attaques par interposition qui voient ou altèrent les données transférées. Les clients et serveurs sont encouragés à prendre en charge des services externes de sécurité des données.

Les protocoles qui n'exigent pas une connexion anonyme explicite sont les plus susceptibles de subir des intrusions étant données certaines techniques communes de mise en œuvre. Précisément, les serveurs Unix qui offrent des connexions d'utilisateur peuvent démarrer initialement comme racine et passer à l'identifiant d'utilisateur approprié après une commande de connexion explicite. Normalement, de tels serveurs refusent toutes les commandes d'accès aux données avant la connexion explicite et peuvent entrer dans un environnement de sécurité restreinte (par exemple, la fonction Unix chroot(2)) pour les utilisateurs anonymes. Si un accès anonyme n'est pas explicitement demandé, la machinerie d'accès aux données est toute entière exposée à des attaques venant de l'extérieur sans avoir une chance de mettre en place des mesures protectrices explicites. Les protocoles qui offrent un accès restreint aux données ne devraient pas permettre un accès

anonyme aux données sans une étape de connexion explicite.

Les considérations générales de sécurité de la [RFC4422] s'appliquent à ce mécanisme. Les considérations de sécurité de la [RFC3454] et les considérations de sécurité de [Unicode] discutées dans la [RFC3454] s'appliquent à ce mécanisme, tout comme celles de la [RFC3629].

6. Considérations relatives à l'IANA

L'entrée du registre "mécanisme SASL" [IANA-SASL] pour le mécanisme ANONYMOUS a été mise à jour par l'IANA pour refléter que c'est maintenant le présent document qui fournit sa spécification technique.

To : iana@iana.org
Sujet : mise à jour de l'enregistrement du mécanisme SASL ANONYMOUS
Nom du mécanisme SASL : ANONYMOUS
Considérations sur la sécurité : Voir la RFC 4505.
Spécification publiée (facultative, recommandée) : RFC 4505
Personnes à contacter pour information : Kurt Zeilenga <Kurt@OpenLDAP.org>
Chris Newman <Chris.Newman@sun.com>
Usage prévu : COMMUN
Auteur/contrôleur des changements : IESG <iesg@ietf.org>
Note : met à jour l'entrée existante pour ANONYMOUS

Le profil "trace" de la [RFC3454] défini pour la première fois dans la présente RFC, a été enregistré :

To : iana@iana.org
Sujet : enregistrement initial du profil "trace" de Stringprep.
Profil Stringprep : trace
Spécification publiée : RFC 4505
Personne & adresse de messagerie à contacter pour information : Kurt Zeilenga <kurt@openldap.org>

7. Remerciements

Le présent document est une révision de la RFC 2245 de Chris Newman. Des portions de la grammaire définie à la Section 1 sont empruntées à la RFC 3629 de François Yergeau.

Ce document a été produit par le groupe de travail SASL de l'IETF.

8. Références normatives

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822, STD 11, *Remplacée par* RFC5322)

[RFC3454] P. Hoffman et M. Blanchet, "Préparation de chaînes internationalisées ("stringprep")", décembre 2002. *(P.S.)*

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003.

[RFC4234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", octobre 2005. *(Remplace* RFC2234, *remplacée par* RFC5234)

[RFC4422] A. Melnikov et K. Zeilenga, éd, "Authentification simple et couche de sécurité (SASL)", juin 2006. *(P.S.)*

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" est défini par "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), amendée par "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) et par "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

9. Références pour information

[RFC3501] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", mars 2003. *(P.S. ; MàJ par* RFC4466, 4469, 4551, 5032, 5182, 7817, 8314, 8437, 8474)

[IANA-SASL] IANA, "SIMPLE AUTHENTICATION AND SECURITY LAYER (SASL) MECHANISMS", <http://www.iana.org/assignments/sasl-mechanisms>.

Appendice A. Changements par rapport à la RFC 2245

Cet appendice n'est pas normatif.

La RFC 2245 permet au client d'inclure des informations de trace facultatives sous la forme d'une chaîne lisbible par l'homme. La RFC 2245 a restreint cette chaîne à l'US-ASCII. Comme l'Internet est international, le présent document utilise une chaîne restreinte aux caractères Unicode codés en UTF-8. Un profil "stringprep" est défini pour préciser quels caractères Unicode sont permis dans cette chaîne. Alors que la chaîne reste limitée à 255 caractères, la longueur codée de chaque caractère peut maintenant aller de 1 à 4 octets.

De plus, un certain nombre de changements rédactionnels ont été faits.

Adresse de l'éditeur

Kurt D. Zeilenga
OpenLDAP Foundation

mél : Kurt@OpenLDAP.org

Déclaration complète de droits de reproduction

droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

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