Groupe de travail Réseau
Request for Comments : 4959
Catégorie : sur la voie de la normalisation
Traduction Claude Brière de L'Isle

R. Siemborski, Google, Inc.
A. Gulbrandsen, Oryx Mail Systems GmbH
septembre 2007

Extension à IMAP pour la réponse initiale de client à l'authentification simple et couche de sécurité (SASL)

Résumé
Aujourd'hui, le protocole d'accès au message Internet (IMAP, *Internet Message Access Protocol*) utilise un profil de l'authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*) qui a toujours exigé au moins un aller retour complet pour une authentification, car il ne prend pas en charge d'argument de réponse initiale de client. Cet aller-retour supplémentaire au début de la session est indésirable, en particulier quand le coût de l'aller-retour est élevé.

Le présent document définit une extension à IMAP qui permet aux clients et serveurs d'éviter cet aller retour en permettant un argument de réponse initiale de client à la commande IMAP AUTHENTICATE.

Table des Matières

1. Introduction

L'extension SASL Réponse initiale de client est présente dans toute mise en œuvre de serveur IMAP [RFC3501] qui retourne "SASL-IR" comme une des ses capacités prises en charge dans sa réponse CAPABILITY.

Les serveurs qui prennent en charge cette extension vont accepter une réponse initiale de client facultative avec la commande AUTHENTICATE pour tout mécanisme SASL [RFC4422] qui la prend en charge.

2. Notation des exigences

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].

Dans les exemples, "C:" et "S:" indiquent les lignes envoyées respectivement par le client et le serveur.

La syntaxe formelle est définie par la [RFC4234] telle qu'étendue par la [RFC3501].

3. Changements à IMAP pour la commande IMAP AUTHENTICATE

Cette extension ajoute un second argument facultatif à la commande AUTHENTICATE qui est définie au paragraphe 6.2.2 de la [RFC3501]. Si ce second argument est présent, il représente le contenu de la "réponse initiale de client" définie au paragraphe 5.1 de la [RFC4422].

Comme avec toute autre réponse de client, cette réponse initiale de client DOIT être codée comme défini à la Section 4 de la [RFC4648]. Elle DOIT aussi être transmise en dehors d'une chaîne entre guillemets ou d'un littéral. Pour envoyer une réponse initiale de longueur zéro, le client DOIT envoyer un seul caractère de bourrage ("="). Cela indique que la réponse est présente, mais qu'elle est une chaîne de longueur zéro.

Lors du décodage des données en BASE64 [RFC4648] dans la réponse initiale de client, les erreurs de décodage DOIVENT être traitées comme IMAP [RFC3501] les traiterait dans toute réponse de client SASL normale. En particulier, le serveur devrait vérifier que ne s'y trouve aucun caractère non explicitement permis par l'alphabet BASE64, ainsi qu'aucune séquence de caractères BASE64 contenant le caractère de bourrage ('=') ailleurs qu'à la fin de la chaîne (par exemple, "=AAA" et "AAA=BBB" ne sont pas permis).

Si le client utilise une réponse initiale avec un mécanisme SASL qui ne prend pas en charge de réponse initiale, le serveur DOIT rejeter la commande avec une réponse marquée BAD.

Note : la prise en charge de l'utilisation de la réponse initiale de client est facultative pour les clients et les serveurs. Les serveurs qui mettent en œuvre cette extension DOIVENT prendre en charge les clients qui omettent la réponse initiale de client, et les clients qui mettent en œuvre cette extension NE DOIVENT PAS envoyer de réponse initiale de client aux serveurs qui n'annoncent pas la capacité SASL-IR. Dans cette situation, les clients DOIVENT revenir au mode compatible IMAP [RFC3501].

Si le client ou le serveur ne prend pas en charge la capacité SASL-IR, un mécanisme qui utilise une réponse initiale de client est négocié en utilisant l'échange de défi/réponse décrit dans la [RFC3501], avec un défi initial du serveur de longueur zéro.

4. Exemples

Voici un exemple d'authentification utilisant le mécanisme PLAIN (voir la [RFC4616]) SASL (sous une couche de protection TLS, voir la [RFC4346]) et une réponse initiale du client :

... le client se connecte au serveur et négocie une couche de protection TLS ...
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN
S: C01 OK Terminé
C: A01 AUTHENTICATE PLAIN dGVzdAB0ZXN0AHRlc3Q=
S: A01 OK Succès (protection TLS)

Noter que même quand un serveur prend en charge cette extension, la négociation suivante (qui n'utilise pas la réponse initiale) est encore valide et DOIT être acceptée par le serveur :

... le client se connecte au serveur et négocie une couche de protection TLS ...
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN
S: C01 OK Terminé
C: A01 AUTHENTICATE PLAIN (noter qu'il y a une espace qui suit le "+" dans la ligne qui suit)
S: +

C: dGVzdAB0ZXN0AHRlc3Q=
S: A01 OK Succès (protection TLS)

Voici un exemple d'authentification utilisant le mécanisme SASL EXTERNAL (défini dans la [RFC4422]) sous une couche de protection TLS (voir la [RFC4346]) et une réponse initiale de client vide :

... le client se connecte au serveur et négocie une couche de protection TLS ...
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN AUTH=EXTERNAL
S: C01 OK Terminé
C: A01 AUTHENTICATE EXTERNAL =
S: A01 OK Succès (protection TLS)

Ceci diffère du traitement d'une telle situation quand une réponse initiale est omise :

... le client se connecte au serveur et négocie une couche de protection TLS ...
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN AUTH=EXTERNAL
S: C01 OK Terminé
C: A01 AUTHENTICATE EXTERNAL (noter qu'il y a une espace qui suit le "+" dans la ligne qui suit)
S: +
C:
S: A01 OK Succès (protection TLS)

5. Considérations relatives à l'IANA

L'IANA a ajouté SASL-IR au registre des capacités IMAP4.

6. Considérations sur la sécurité

L'extension définie dans le présent document est soumise à de nombreuses considérations de sécurité définies dans les [RFC3501] et [RFC4422].

Les mises en œuvre de serveur DOIVENT traiter l'omission d'une réponse initiale de client de la commande AUTHENTICATE comme défini par la [RFC3501] (comme si cette extension n'existait pas).

Bien que la [RFC3501] n'ait pas exprimé de limitation de longueur de ligne, certaines mises en œuvre ont choisi d'en appliquer quand même. Ces mises en œuvre DOIVENT être conscientes que l'ajout du paramètre Réponse initiale à AUTHENTICATE peut augmenter la longueur maximale de ligne que les analyseurs IMAP peuvent s'attendre à prendre en charge. Les mises en œuvre de serveurs DOIVENT être capables de recevoir la plus grande réponse initiale de client possible que les mécanismes qu'ils prennent en charge peuvent recevoir.

7. Syntaxe formelle

La spécification de syntaxe suivante utilise la notation de forme Backus-Naur augmenté [RFC4234]. La [RFC3501] définit la capacité de non terminal, auth-type *(type d'authentification)* et base64.

```
capability =/ "SASL-IR"

authenticate  = "AUTHENTICATE" SP auth-type [SP (base64 / "=")]
                *(CRLF base64)
;; redéfinit le AUTHENTICATE de la [RFC3501]
```

8. Remerciements

Les auteurs tiennent à remercier de leurs contributions Ken Murchison et Mark Crispin, ainsi que le reste du groupe de travail IMAPEXT pour leur assistance dans la révision de ce document. Alexey Melnikov et Cyrus Daboo ont aussi participé à des discussions sur cette extension.

9. Références

9. 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)

[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)

[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.)*

[RFC4648] S. Josefsson, "Codages de données Base16, Base32 et Base64", octobre 2006. (*Remplace* RFC3548) *(P.S.)*

9.2 Références pour information

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

[RFC4616] K. Zeilenga, éd., "Mécanisme PLAIN de l'authentification simple et couche de sécurité (SASL)", août 2006. *(P.S.)*

Adresse des auteurs

Robert Siemborski
Google, Inc.
1600 Ampitheatre Parkway
Mountain View, CA 94043
téléphone : +1 650 623 6925
mél : robsiemb@google.com

Arnt Gulbrandsen
Oryx Mail Systems GmbH
Schweppermannstr. 8
D-81671 Muenchen
Germany
mél : arnt@oryx.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres 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 actuellement fourni par la Internet Society.