Groupe de travail Réseau
Request for Comments : 2195
Catégorie : En cours de normalisation
RFC rendue obsolète : 2095
Traduction Claude Brière de L'Isle

J. Klensin
R. Catoe
P. Krumviede
MCI
septembre 1997

Extension IMAP/POP AUTHorize pour simple mise au défi/réponse

Résumé
Bien que IMAP4 prenne en charge un certain nombre de forts mécanismes d'authentification, comme décrits dans la [RFC1731], il lui manque un mécanisme qui ne passe ni les mots de passe réutilisables en texte en clair à travers le réseau, ni n'exige une infrastructure de sécurité significative ou que le serveur de messagerie mette à jour un fichier d'authentification au dimension du système de messagerie sur chaque accès de messagerie. La présente spécification fournit un protocole d'authentification par simple mise au défi-réponse dont l'utilisation convient avec IMAP4. Comme il utilise des résumés à clés MD5 et n'exige pas que le secret soit mémorisé en clair sur le serveur, il peut aussi constituer une amélioration de APOP pour l'utilisation de POP3, comme spécifié dans la [RFC1734].

1. Introduction

Les normes proposées existantes spécifient un mécanisme AUTHENTICATE pour le protocole IMAP4 [RFC2060], [RFC1731] et un mécanisme AUTH parallèle pour le protocole POP3 [RFC1734]. Le mécanisme AUTHENTICATE est destiné à être extensible ; les quatre méthodes spécifiées dans la [RFC1731] sont toutes très puissantes et exigent une certaine infrastructure de sécurité pour leur prise en charge. La spécification POP3 de base [RFC1939] contient aussi un mécanisme léger de mise au défi-réponse appelé APOP. APOP est associé à la plupart des risques qui découlent de tels protocoles : en particulier, il exige que les deux machines client et serveur aient accès au secret partagé en clair. CRAM offre une méthode pour éviter de telles mémorisations en clair tout en conservant la simplicité de l'algorithme de APOP en utilisent seulement MD5, mais dans une méthode "à clés".

À présent, il manque à IMAP [RFC2060] une facilité correspondant à APOP. La seule solution de remplacement aux forts mécanismes identifiés dans la [RFC1731] est la prise en charge à travers la commande LOGIN de la [RFC2060] du nom d'utilisateur et du mot de passe vraisemblablement en clair. Le présent document décrit un mécanisme simple de mise au défi-réponse, similaire à APOP et au CHAP de PPP [RFC1334],qui peut être utilisé avec IMAP (et, en principe, avec POP3).

Ce mécanisme présente aussi l'avantage sur certaines solutions de remplacement possibles de ne pas exiger que le serveur conserve les informations sur les "connexions" de messagerie connexion par connexion. Bien que les mécanismes qui exigent l'enregistrement d'un tel historique par connexion puissent offrir des protocoles à la sécurité améliorée, les protocoles comme IMAP, qui peut avoir plusieurs connexions ouvertes plus ou moins simultanément entre un client et un serveur donnés, peuvent rendre leur mise en œuvre particulièrement difficile.

2. Mécanisme d'authentification par mise au défi - réponse (CRAM)

(CRAM, *Challenge-Response Authentication Mechanism*)

Le type d'authentification associé à CRAM est "CRAM-MD5".

Les données codées dans la première réponse prête contiennent une chaîne vraisemblablement arbitraire de chiffres aléatoires, un horodatage, et le nom principal pleinement qualifié du serveur. La syntaxe de la forme non codée doit correspondre à celle d'un "msg-id" de la [RFC0822] comme décrit dans la [RFC1939].

Le client prend note des données puis répond avec une chaîne comportant le nom d'utilisateur, une espace, et un "résumé". Ce dernier est calculé en appliquant l'algorithme MD5 chiffré tiré de la [RFC2104] où la clé est un secret partagé et le texte

résumé est l'horodatage (y compris les crochets angulaires).

Ce secret partagé est une chaîne qui n'est connue que du client et de serveur. Le paramètre "résumé" lui-même est une valeur de 16 octets qui est envoyée en format hexadécimal, en utilisant des caractères ASCII minuscules.

Lorsque le serveur reçoit cette réponse du client, il vérifie le résumé fourni. Si il est correct, le serveur devrait considérer que le client est authentifié et répondre en conséquence.

Le MD5 chiffré est choisi pour cette application à cause de la plus grande sécurité qui est réservée à l'authentification des messages courts. De plus, l'utilisation des techniques décrites dans la [RFC2104] pour le calcul anticipé des résultats intermédiaires rend possible d'éviter la mémorisation de texte explicitement en clair du secret partagé sur le système du serveur en mémorisant à la place les résultats intermédiaires qui sont appelés des "contextes".

CRAM ne prend pas en charge de mécanisme de protection.

Exemple :

Les exemples du présent document montrent l'utilisation du mécanisme CRAM avec la commande AUTHENTICATE de IMAP4 [RFC1731]. Le codage en base64 des mises au défi et des réponses fait partie de la commande IMAP4 AUTHENTICATE, et ne fait pas partie de la spécification CRAM elle-même.

S: * OK IMAP4 Server
C: A0001 AUTHENTICATE CRAM-MD5
S: + PDE4OTYuNjk3MTcwOTUyQHBvc3RvZmZpY2UucmVzdG9uLm1jaS5uZXQ+
C: dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWI0ZTZlNzMzNGQzODkw
S: A0001 OK authentification CRAM réussie

Dans cet exemple, le secret partagé est la chaîne "tanstaaftanstaaf". Donc, le résumé MD5 chiffré est produit en calculant

MD5((tanstaaftanstaaf XOR opad),
    MD5((tanstaaftanstaaf XOR ipad),
    <1896.697170952@postoffice.reston.mci.net>))

où ipad et opad sont comme défini dans le MD5 chiffré de la [RFC2104] et la chaîne montrée dans le défi est le codage en base64 de <1896.697170952@postoffice.reston.mci.net>. Le secret partagé est bourré de zéros jusqu'à une longueur de 64 octets. Si le secret partagé fait plus de 64 octets, le résumé MD5 du secret partagé est utilisé comme une entrée de 16 octets dans le calcul du MD5 chiffré.

Cela donne une valeur de résumé (en hexadécimal) de "b913a602c7eda7a495b4e6e7334d3890".

Le nom d'utilisateur est alors ajouté devant lui, formant "tim b913a602c7eda7a495b4e6e7334d3890".

Qui est alors codé en base64 pour satisfaire aux exigences de la commande IMAP4 AUTHENTICATE (ou de la commande POP3 AUTH similaire) donnant "dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWI0ZTZlNzMzNGQzODkw".

3. Références

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC1334] B. Lloyd et W. Simpson, "Protocoles d'authentification PPP", octobre 1992. *(Remplacé par RFC1994)*

[RFC1731] J. Myers, "Mécanismes d'authentification IMAP4", décembre 1994.*(P.S.)*

[RFC1734] J. Myers, "Commande POP3 AUTHentification", décembre 1994. *(P.S., remplacée par la RFC5034)*

[RFC1939] J. Myers, M. Rose, "Protocole Post Office - version 3", mai 1996. (*MàJ par* RFC1957, RFC2449) (STD0053)

[RFC2060] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", décembre 1996. *(Remplace* RFC1730) (*Obsolète, voir* RFC3501) *(P.S.)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

4. Considérations pour la sécurité

On estime que le mécanisme d'authentification CRAM assure l'identification de l'origine et la protection contre la répétition pour une session. En conséquence, un serveur qui met en œuvre à la fois une commande de mot de passe en clair et ce type d'authentification ne devrait pas permettre les deux méthodes d'accès pour un utilisateur.

Bien que la sauvegarde, sur le serveur, des "contextes" (voir à la section 2) soit en fin de compte meilleure que de sauvegarder les secrets partagés en clair comme l'exigent CHAP [RFC1334] et APOP [RFC1939], il ne sert à rien de protéger les secrets si le serveur lui-même est compromis. Par conséquent, les serveurs qui mémorisent les secrets et les contextes doivent tous deux être protégés à un niveau approprié à la valeur des informations qui peuvent être contenues dans les boîtes aux lettres et les identités des utilisateurs.

Lorsque la longueur du secret partagé augmente, s'accroît aussi la difficulté de le déduire.

Bien qu'il soit maintenant suggéré dans la littérature que l'utilisation de MD5 et de MD5 chiffré dans les procédures d'authentification a probablement une durée de vie efficace limitée, la technique est maintenant largement déployée et comprise. On estime que la compréhension générale peut aider, avec le remplacement rapide par CRAM-MD5, des utilisations actuelles de mots de passe permanents en clair dans IMAP. Le présent document a été délibérément écrit pour permettre une mise à niveau facile avec l'utilisation de SHA (ou de toute solution de remplacement qui pourrait émerger) lorsque elle sera considérée comme étant largement disponible et d'une sûreté adéquate.

Même avec l'utilisation de CRAM, les usagers sont encore vulnérables aux attaques actives. Un exemple d'une attaque active de plus en plus courante est la "capture de session TCP" décrite dans l'avis du CERT CA-95:01 [CERT95].

Voir des précisions à la section 1 ci-dessus.

5. Remerciements

Le présent mémoire emprunte largement les idées et le texte des [RFC1939] et [RFC1731] et des remerciements sont dus aux auteurs de ces documents. Ran Atkinson a fait un certain nombre de précieuses contributions techniques et rédactionnelles au présent document.

6. Adresse des auteurs

John C. Klensin
MCI Telecommunications
800 Boylston St, 7th floor
Boston, MA 02199
USA
mél : klensin@mci.net
téléphone : +1 617 960 1011

Randy Catoe
MCI Telecommunications
2100 Reston Parkway
Reston, VA 22091
USA
mél : randy@mci.net
téléphone : +1 703 715 7366

Paul Krumviede
MCI Telecommunications
2100 Reston Parkway
Reston, VA 22091
USA
mél : paul@mci.net
téléphone : +1 703 715 7251