

Groupe de travail Réseau
Request for Comments: 2444
RFC mise à jour : 2222
Catégorie : En cours de normalisation

C. Newman, Innosoft
octobre 1998
Traduction Claude Brière de L'Isle

Mécanisme SASL de mot de passe à utilisation unique

Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright

Copyright (C) The Internet Society (1998). Tous droits réservés.

Résumé

OTP [RFC2289] fournit un mécanisme d'authentification utile pour les situations où la confiance envers le client ou le serveur est limitée. Actuellement, OTP est ajouté aux protocoles de façon ad hoc avec une analyse heuristique. La présente spécification définit un mécanisme OTP SASL [RFC2222] afin qu'il soit facilement et formellement intégré dans de nombreux protocoles d'application.

1. Comment lire ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE" et "PEUT" dans ce document sont à interpréter comme défini dans la [RFC2119].

Le présent mémoire suppose que le lecteur est familiarisé avec OTP [RFC2289], les réponses étendues OTP [RFC2243] et SASL [RFC2222].

2. Utilisation prévue

Le mécanisme OTP SASL remplace le mécanisme SKEY SASL [RFC2222]. OTP est un bon choix pour les scénarios d'utilisation où le client est de confiance (par exemple, un client kiosque) car un mot de passe à utilisation unique va donner au client une seule opportunité d'agir au nom de l'utilisateur. OTP est aussi un bon choix pour les situations où des connexions interactives sont permises au serveur, car une base de données d'authentification OTP compromise n'est soumise qu'à des attaques de dictionnaire, à la différence des bases de données d'authentification pour d'autres mécanismes simples comme CRAM-MD5 [RFC2195]. Il est important de noter que chaque utilisation du mécanisme OTP cause la mise à jour de l'entrée de la base de données d'authentification pour un utilisateur.

Ce mécanisme SASL donne un moyen formel d'intégrer OTP dans les protocoles à capacité SASL, y compris IMAP [RFC2060], ACAP [RFC2244], POP3 [RFC1734] et LDAPv3 [RFC2251].

3. Profil d'OTP pour SASL

OTP [RFC2289] et les réponses OTP étendues [RFC2243] offrent un certain nombre d'options. Cependant, pour que l'authentification réussisse, le client et le serveur ont besoin d'ensembles d'options compatibles. La présente spécification définit un seul mécanisme SASL : OTP. Les règles suivantes s'appliquent à ce mécanisme :

- o La syntaxe de réponse étendue DOIT être utilisée.
- o Les serveurs DOIVENT prendre en charge les quatre réponses OTP étendues suivantes : "hex", "word", "init-hex" et "init-word". Les serveurs DOIVENT prendre en charge les réponses "word" et "init-word" pour le dictionnaire standard et DEVRAIENT prendre en charge des dictionnaires de remplacement. Les serveurs NE DOIVENT PAS exiger l'utilisation d'extensions ou options OTP supplémentaires.
- o Les clients DEVRAIENT prendre en charge l'affichage du défi OTP à l'utilisateur et l'entrée d'un OTP en format multi mots. Les clients PEUVENT aussi prendre en charge l'entrée directe de la phrase de passe et du calcul de la réponse "hex" ou "word".

- o Les clients DOIVENT indiquer quand l'authentification échoue à cause d'un numéro de séquence qui devient trop faible et DEVRAIENT offrir à l'utilisateur l'option de rétablir la séquence en utilisant la réponse "init-hex" ou "init-word".

La prise en charge de l'algorithme MD5 est EXIGÉE, et la prise en charge de l'algorithme SHA1 est RECOMMANDÉE.

4. Mécanisme OTP d'authentification

Le mécanisme ne fournit aucune couche de sécurité.

Le client commence par envoyer un message au serveur, contenant les deux éléments d'information suivants.

- (1) Une identité d'autorisation. Lorsque on utilise la chaîne vide, c'est l'identité d'authentification par défaut. C'est utilisé par les administrateurs de système ou les serveurs mandataires pour se connecter avec une identité d'utilisateur différente. Ce champ peut faire jusqu'à 255 octets et se termine par un octet NUL (0). Les caractères US-ASCII imprimables sont préférés, bien que les caractères UTF-8 [RFC2279] imprimables soient permis pour la prise en charge des noms internationaux. L'utilisation de jeux de caractères autres que US-ASCII et UTF-8 est interdite.
- (2) Une identité d'authentification. L'identité dont la phrase de passe sera utilisée. Ce champ peut faire jusqu'à 255 octets. Les caractères US-ASCII imprimables sont préférés, bien que les caractères UTF-8 [RFC2279] imprimables soient permis pour la prise en charge des noms internationaux. L'utilisation de jeux de caractères autres que US-ASCII et UTF-8 est interdite.

Le serveur répond par l'envoi d'un message contenant le défi OTP tel que décrit dans OTP [RFC2289] et les réponses OTP étendues [RFC2243].

Si un client voit un nom d'algorithme de hachage inconnu, il ne sera pas capable de traiter une phrase de passe entrée par l'usager. Dans cette situation, le client PEUT inviter à passer au format six-mots, produire la séquence d'annulation comme spécifié par le profil SASL pour le protocole utilisé et essayer un mécanisme SASL différent, ou clore la connexion et refuser l'authentification. Il résulte de ce comportement qu'un serveur est limité à un algorithme de hachage d'OTP par usager.

En cas de succès, le client génère une réponse étendue dans le format "hex", "word", "init-hex" ou "init-word". Le client n'est pas obligé de terminer la réponse par une espace ou une nouvelle ligne et NE DEVRAIT PAS inclure d'espaces inutiles.

Les serveurs DOIVENT tolérer des entrées de longueur arbitraire, mais PEUVENT faire échouer l'authentification si la longueur de l'entrée du client excède une taille raisonnable.

5. Exemples

Dans ces exemple, "C:" représente les lignes envoyées du client au serveur et "S:" représente les lignes envoyées du serveur au client. Le nom de l'usager est "tim" et aucune identité d'autorisation n'est fournie. Le "<NUL>" ci-dessous représente un octet ASCII NUL.

Ce qui suit est un exemple du mécanisme d'OTP utilisant le profil ACAP [RFC2244] de SASL. La phrase de passe utilisée dans cet exemple est : This is a test (*Ceci est un essai*).

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-md5 499 ke1234 ext"
C: "hex:5bf075d9959d036f"
S: a001 OK "AUTHENTIFICATION terminée"
```

Voici le même exemple en utilisant la réponse six-mots :

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-md5 499 ke1234 ext"
C: "word:BOND FOGY DRAB NE RISE MART"
S: a001 OK "AUTHENTIFICATION terminée"
```

Voici le même exemple en utilisant le mécanisme OTP-SHA1 :

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-sha1 499 ke1234 ext"
C: "hex:c90fc02cc488df5e"
S: a001 OK "AUTHENTIFICATION terminée"
```

Voici le même exemple avec la réponse étendue init-hex :

```
C: a001 AUTHENTICATE "OTP" {4}
C: <NUL>tim
S: + "otp-md5 499 ke1234 ext"
C: "init-hex:5bf075d9959d036f:md5 499 ke1235:3712dcb4aa5316c1"
S: a001 OK "séquence OTP réinitialisée, authentification terminée"
```

Ce qui suit est un exemple du mécanisme OTP qui utilise le profil IMAP [RFC2060] de SASL. La phrase de passe utilisée dans cet exemple est : this is a test

```
C: a001 AUTHENTICATE OTP
S: +
C: AHRpbQ==
S: + b3RwLW1kNSAxMjMga2UxMjM0IGV4dA==
C: aGV4OjExZDRjMTQ3ZTIyN2MxZjE=
S: a001 OK AUTHENTIFICATION terminée
```

Noter que le manque d'une réponse client initiale et le codage base64 sont caractéristiques du profil IMAP de SASL. Le défi du serveur est "otp-md5 123 ke1234 ext" et la réponse du client est "hex:11d4c147e227c1f1".

6. Considérations pour la sécurité

La présente spécification n'introduit pas de considérations de sécurité au delà de celles décrites dans SASL [RFC2222], OTP [RFC2289] et les réponses OTP étendues [RFC2243]. Un bref résumé de ces considérations suit :

Ce mécanisme n'assure pas la confidentialité de session, l'authentification du serveur ni la protection contre les attaques actives.

Ce mécanisme est sujet à des attaques passives de dictionnaire. La sévérité de ces attaques peut être réduite par un bon choix des phrases de passe.

La base de données d'authentification de serveur qu'il est nécessaire d'utiliser avec OTP n'a pas besoin d'être équivalente au texte en clair.

Les mises en œuvre de serveur DOIVENT se protéger contre l'attaque de mise en concurrence de la [RFC2289].

7. Considérations multinationales

Comme l'accès à distance est un service d'importance cruciale, les usagers sont encouragés à restreindre les noms d'utilisateur et les phrases de passe au jeu de caractères US-ASCII. Cependant, si des caractères en dehors du jeu de caractères US-ASCII sont utilisés dans les noms d'utilisateur et les phrases de passe, ils sont alors interprétés selon UTF-8 [RFC2279].

La prise en charge par le serveur d'autres dictionnaires est fortement RECOMMANDÉE pour permettre l'utilisation du format six-mots avec des mots non anglais.

8. Considérations relatives à l'IANA

Voici le gabarit d'enregistrement pour le mécanisme OTP SASL :

Nom du mécanisme SASL : OTP

Considérations de sécurité : Voir la section 6 de ce mémoire

Spécification publiée : Le présent mémoire

Adresse personnelle & de messagerie à contacter pour des informations complémentaires : Voir l'adresse de l'auteur ci-dessous

Utilisation prévue : COMMUNE

Auteur/contrôleur des changements : Voir l'adresse de l'auteur ci-dessous

Le présent mémoire amende aussi l'enregistrement du mécanisme SKEY SASL [RFC2222] en changeant son utilisation prévue en OBSOLÈTE.

9. Références

- [RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992. (*Information*)
- [RFC1734] J. Myers, "Commande POP3 AUTHentification", décembre 1994. (*P.S., remplacée par la RFC5034*)
- [RFC2060] M. Crispin, "Protocole d'[accès au message Internet](#) - version 4rev1", décembre 1996. (*Remplace RFC1730 (Obsolète, voir RFC3501) (P.S.)*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2195] J. Klensin et autres, "[Extension IMAP/POP AUTHorize](#) pour mise au défi/réponse simple", septembre 1997. (*P.S.*)
- [RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir RFC4422, RFC4752 (MàJ par RFC2444) (P.S.)*)
- [RFC2243] C. Metz, "[Réponses OTP étendues](#)", novembre 1997. (*P.S.*)
- [RFC2244] C. Newman, J. G. Myers, "[ACAP – Protocole d'accès à la configuration d'application](#)", novembre 1997. (*P.S.*)
- [RFC2251] M. Wahl, T. Howes et S. Kille, "[Protocole léger d'accès à un répertoire](#) (v3)", décembre 1997.
- [RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir RFC3629) (D.S.)*)
- [RFC2289] N. Haller, C. Metz, P. Nesser, M. Straw, "Système de [mot de passe à utilisation unique](#)", février 1998. ([STD0061](#))

10. Adresse de l'auteur

Chris Newman
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790
USA
mél : chris.newman@innosoft.com

11. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1998). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les copyrights définis dans les processus de normes pour Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et L'INTERNET SOCIETY et L'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation des informations présentées ici n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.