Groupe de tavail Réseau
Request for Comments : 2243
Catégorie : En cours de normalisation

C. Metz, The Inner Net
novembre 1997
Traduction Claude Brière de L'Isle

Réponses OTP étendues

Résumé
Le présent document fournit une spécification pour un type de réponse à un défi OTP *(One-Time Password, mot de passe à utilisation unique)* [RFC1938] qui porte une indication explicite du codage de la réponse. On présente les codages pour les deux formats de données OTP obligatoires qui utilisent ce nouveau type de réponse.

Le présent document fournit aussi la spécification pour une réponse qui permet à un générateur OTP de demander qu'un serveur réinitialise une séquence et change des paramètres tels qu'une phrase de passe secrète.

1. Conventions, termes, et notation

Le présent document spécifie les formats de données et les comportements logiciels nécessaires pour utiliser les réponses OTP étendues. Les formats de données sont décrits de trois façons : en utilisant une syntaxe de style de page manuelle UNIX ad hoc, en utilisant le BNF augmenté décrit aux sections 2 et 3 de la [RFC0822], et par des exemples. Si il devait y avoir conflit entre ces descriptions, le BNF augmenté l'emporterait. Les comportements de logiciel sont décrits par des mots, et les exigences spécifiques de conformité de comportement sont précisées en utilisant la terminologie des exigences (précisément, les mots DOIT, DEVRAIT, et PEUT) définis dans la [RFC2119].

2. Défis et réponses étendus

Le présent document s'appuie sur le protocole et la terminologie spécifiés dans la [RFC1938] et suppose que le lecteur est déjà familiarisé avec ce document et en comprend le contenu.

Un défi étendu est une seule ligne de texte imprimable terminé soit par une nouvelle ligne suivante appropriée pour le contexte de son utilisation (par exemple, un CR ASCII suivi par un LF ASCII) ou un caractère espace. Il contient un défi OTP standard, un caractère espace, et une liste qu'utilisent les générateurs pour déterminer quelles réponses étendues sont prises en charge par un serveur.

Une réponse étendue est une seule ligne de texte imprimable terminée par une nouvelle ligne suivante appropriée pour le contexte de son utilisation. Elle contient deux jetons ou plus qui sont séparés par un seul caractère deux-points (':'). Le premier jeton contient un spécificateur de type qui indique le format du reste de la réponse. Les jetons qui suivent sont des données d'argument pour la réponse OTP étendue. Au moins un jeton de données DOIT être présent.

2.1 Syntaxe

Dans la syntaxe de type page manuelle UNIX, la forme générale d'un défi étendu pourrait être décrite comme :

<défi OTP standard> ext[,<identifiant d'ensemble d'extension>[, ...]]

Et la forme générale d'une réponse étendue pourrait être décrite par :

<spécificateur-de-type>:<arg1>[:<arg2>[:...]]

En syntaxe BNF augmenté, la syntaxe de la forme générale d'un défi étendu et d'une réponse étendue est :

```
défi-étendu              = défi-otp 1*caractère-LWSP liste-de-capacités (NL / *caractère-LWSP)
défi-otp                 = <défi OTP standard>
liste-de-capacités       = "ext" *("," identifiant-d'ensemble-d'extensions)
identifiant-d'ensemble-d'extensions  = *<tout CARACT sauf LWSP, CTL, ou ",">
réponse-étendue          = type 1*(":" argument) NL
type                     = jeton
argument                 = jeton
jeton                    = 1*<tout CARACT sauf ":" et CTL>
NL                       = <nouvelle ligne suivante appropriée pour le contexte d'utilisation d'OTP>
```

Un exemple de défi étendu indiquant la prise en charge des réponses OTP étendues pour un ensemble mythique de réponses "foo" est :

```
otp-md5 123 mi1234 ext,foo
```

Un exemple de réponse étendue utilisant un type mythique nommé "foo" est :

```
foo:des données:encore plus de données:12345
```

2.2 Exigences

Un serveur qui se conforme à la présente spécification :

1. DOIT être capable de recevoir et analyser la forme générale d'une réponse étendue ;
2. DOIT être capable de recevoir, analyser, et traiter correctement toutes les réponses étendues spécifiées dans ce document ;
3. DOIT traiter le champ Type de façon insensible à la casse ;
4. DOIT rejeter toute tentative d'authentification qui utilise une réponse étendue si il ne prend pas en charge ce type de réponse ;
5. DEVRAIT fournir au générateur une indication appropriée si la réponse a été rejetée à cause de (4) ;
6. DOIT limiter raisonnablement la longueur de l'entrée ;
7. DOIT accepter autrement des quantités arbitraires d'espaces blanches chaque fois qu'une réponse le permet ;
8. DOIT être capable de recevoir et traiter correctement les réponses OTP standard.

Un générateur conforme à la présente spécification :

1. DOIT être capable de générer des réponses OTP standard ;
2. DOIT utiliser des réponses standard sauf si un défi étendu a été reçu du serveur ET du germe particuliers ;
3. DOIT générer le champ Type en minuscules ;
4. NE DOIT PAS envoyer un type de réponse pour lequel le serveur n'a pas indiqué sa prise en charge au moyen d'un défi étendu.

Les identifiants d'ensemble d'extension et les identifiants de type d'extension désignés par le préfixe "x-" sont réservés pour des utilisations privées dans des mises en œuvre mutuellement consentantes. Les mises en œuvre qui ne reconnaissent pas une extension "x-" particulière DOIVENT ignorer cette extension. Cela signifie que toutes les extensions "x-" ont des chances de ne pas être inter opérables avec les autres extensions. Une considération attentive devrait être apportée à la possibilité qu'un serveur interagisse avec une mise en œuvre de générateur qui, bien qu'elle reconnaisse une certaine extension "x-", l'utilise pour un objet différent. Tout l'espace de noms d'extension restant est réservé à l'IANA, qui n'allouera officiellement d'extension dans cet espace de nom qu'après son approbation par l'IESG. Tant que subsistera le groupe de travail OTP, il est recommandé que l'IESG le consulte avant d'approuver une telle allocation.

3. Réponses "hex" et "word"

Il existe un cas très rare dans lequel une réponse OTP standard pourrait être un codage valide dans les deux formats hexadécimal et de six mots. Un exemple en est la réponse "ABE ACE ADA ADD BAD A". La solution à ce problème, qui est rendue obligatoire par la spécification OTP, est que les serveurs conformes DOIVENT tenter d'analyser et vérifier une réponse standard dans les deux formats hexadécimal et six mots, et doit considérer que l'authentification est réussie si l'une ou l'autre réussit.

Ce problème peut être facilement résolu en utilisant les réponses étendues. La réponse "hex" et la réponse "word" sont deux types de réponses qui codent un OTP dans une réponse étendue qui décrit explicitement le codage. Ces réponses

commencent par une étiquette de type de "hex" pour un OTP hexadécimal et de "word" pour un OTP codé en six mots. Ces réponses contiennent un champ d'argument qui contient une réponse OTP standard codée dans le format indiqué.

3.1 Syntaxe

Dans la syntaxe de style page manuelle UNIX, le format de ces réponses pourrait être décrit par :

hex :<nombre hexadécimal>
word :<six mots du dictionnaire>

En syntaxe BNF augmenté et avec les définitions déjà fournies, la syntaxe de ces réponses est :

```
hex-response  = "hex:" hex-64bit NL
hex-64bit     = 16(hex-char *LWSP-char)
hex-char      = ("A" / "B" / "C" / "D" / "E" / "F" / "a" / "b" / "c" / "d" / "e" / "f" / "0" / "1" / "2" / "3" / "4" / "5" / "6" /
                "7" / "8" / "9")

word-response = "word:" word-64bit NL
word-64bit    = 6(otp-word 1*LWSP-char)
otp-word      = <tout mot valide du dictionnaire de codage d'OTP standard>
```

Des exemples de ces réponses sont :

hex:8720 33d4 6202 9172
word:VAST SAUL TAKE SODA SUCH BOLT

3.2 Exigences

Un serveur conforme à la présente spécification :
1. DOIT traiter tous les arguments de façon insensible à la casse.

Un générateur conforme à la présente spécification :
1. DEVRAIT générer des jetons otp-word en majuscules avec une seule espace pour les séparer ;
2. DEVRAIT générer des nombres hexadécimaux en utilisant seulement des minuscules comme lettres.

4. Réponses "init-hex" et "init-word"

La spécification OTP exige que les mises en œuvre donnent aux clients un moyen pour réinitialiser ou changer ses informations d'OTP avec un serveur mais elle n'exige pas de protocole spécifique pour le faire. Les mises en œuvre qui prennent en charge les réponses OTP étendues décrites dans le présent document DOIVENT prendre en charge la réponse avec les spécificateurs de type "init-hex" et "init-word", qui assurent un moyen standard pour qu'un client réinitialise ses informations d'OTP avec un serveur. Cette réponse est destinée à être utilisée seulement par des clients automatisés. À cause de cela, la forme recommandée de cette réponse utilise le codage hexadécimal pour les données binaires. Il est possible à un usager de taper une réponse "init-hex" ou "init-word".

4.1 Syntaxe

En syntaxe de style page manuelle UNIX, le format de ces réponses pourrait être décrit par :

init-hex:<OTP-actuel>:<nouveaux-paramètres>:<nouvel-OTP>
init-word:<OTP-actuel>:<nouveaux-paramètres>:<nouvel-OTP>

En syntaxe BNF augmenté et avec les définitions déjà fournies, la syntaxe de la réponse "init-hex" est :

```
init-hex-response =          "init-hex:" OTP-actuel ":" nouveaux-paramètres ":" nouvel-OTP NL

OTP-actuel          = hex-64bit
nouvel-OTP          = hex-64bit
nouveaux-paramètres = algorithme ESPACE numéro-de-séquence ESPACE germe
algorithme          = "md4" / "md5" / "sha1"
```

numéro-de-séquence = 4*3CHIFFRE
germe = 16*1(ALPHA / CHIFFRE)

En syntaxe BNF augmenté et avec les définitions déjà fournies, la syntaxe de la réponse "init-word" est :

init-word-response = "init-word:" OTP-actuel ":" nouveaux-paramètres ":" nouvel-OTP NL

OTP-actuel = word-64bit
nouvel-OTP = word-64bit

nouveaux-paramètres = algorithme ESPACE numéro-de-séquence ESPACE germe
algorithme = "md4" / "md5" / "sha1"
numéro-de-séquence = 4*3CHIFFRE
germe = 16*1(ALPHA / CHIFFRE)

Noter que tous les champs appropriés pour la réponse "init-hex" DOIVENT être codés en hexadécimal et que tous les champs appropriés pour la réponse "init-word" DOIVENT être codés en six-mots.

Des exemples de ces réponses sont :

init-hex:f6bd 6b33 89b8 7203:md5 499 ke6118:23d1 b253 5ae0 2b7e
init-hex:c9b2 12bb 6425 5a0f:md5 499 ke0986:fd17 cef1 b4df 093e

init-word:MOOD SOFT POP COMB BOLO LIFE:md5 499 ke1235:
ARTY WEAR TAD RUG HALO GIVE
init-word:END KERN BALM NICK EROS WAVY:md5 499 ke1235:
BABY FAIN OILY NIL TIDY DADE

(Noter que toutes ces réponses sont sur une ligne. Du fait de leur longueur, elles ont dû être étalées sur plusieurs lignes afin d'être incluses ici. Ces réponses NE DOIVENT PAS s'étendre sur plus d'une ligne en utilisation réelle.)

4.2 Description des champs

Le champ OTP-actuel contient la réponse [RFC1938] au défi OTP. Le champ nouveaux-paramètres contient les paramètres pour le nouveau défi demandé par le client et le champ nouvel-OTP contient une réponse à ce défi. Si la réinitialisation ne réussit pas, un serveur DOIT mémoriser le nouvel OTP dans sa base de données comme étant le dernier OTP réussi reçu et le numéro de séquence dans le prochain défi présenté par le serveur DOIT être de un de moins que le numéro de séquence spécifié dans le champ nouveaux-paramètres.

Le champ nouveaux-paramètres est haché comme une chaîne de la même façon que le serait un germe ou une phrase de passe secrète. Toutes les valeurs des autres champs sont hachées sous leur forme binaire non codée, dans l'ordre des octets du réseau et sans aucun bourrage.

4.3 Exigences

Un serveur conforme à la présente spécification :
1. NE DEVRAIT PAS permettre à un usager d'utiliser la même valeur pour son germe et pour la phrase de passe secrète.
2. DOIT désactiver tous les accès OTP à tout principal dont le numéro de séquence serait inférieur à un.
3. DOIT décrémenter le numéro de séquence si une réponse de réinitialisation comporte un OTP-actuel valide, mais si le serveur n'est pas capable de réussir à traiter pour une raison quelconque les nouveaux-paramètres ou le nouvel-OTP.

Un générateur conforme à la présente spécification :
1. NE DEVRAIT PAS permettre à un usager d'utiliser la même valeur pour son germe et pour la phrase de passe secrète.
2. DOIT prendre des mesures spécifiques pour empêcher des boucles infinies de tentatives de réinitialisation en cas d'échec.
3. DEVRAIT fournir à l'usager des indications sur le fait que la réinitialisation a lieu.
4. NE DEVRAIT PAS faire une réinitialisation sans la permission de l'usager, soit pour cette instance spécifique, soit comme option de configuration.
5. NE DEVRAIT PAS réessayer une réinitialisation qui a échoué sans la permission de l'usager.
6. DEVRAIT avertir l'usager si le numéro de séquence tombe en dessous de dix.
7. DOIT refuser de générer des OTP avec un numéro de séquence inférieur à un.

5. Considérations pour la sécurité

Toutes les considérations de sécurité pour le système OTP s'appliquent aussi au système OTP avec réponses étendues.

Ces réponses étendues, comme OTP lui-même, ne protègent pas l'usager contre les attaques actives. L'en-tête d'authentification IPsec [RFC1826] (ou une autre technique avec une force au moins égale à celle de IPsec AH) DEVRAIT être utilisée pour se protéger contre de telles attaques.

Les conséquences d'une attaque active réussie sur la réponse de réinitialisation peuvent être plus sévères que de simplement capturer une seule session. Un attaquant pourrait substituer sa propre réponse à celle de l'usager légitime. L'attaquant peut alors être capable d'utiliser le système d'OTP pour s'authentifier à volonté lui-même comme étant l'usager (au moins jusqu'à ce qu'il soit détecté).

L'échec à mettre en œuvre l'exigence 3 du serveur du paragraphe 4.3 ouvre une mise en œuvre à une attaque fondée sur la répétition de la partie OTP-actuel de la réponse.

6. Remerciements

Comme la RFC1938, le protocole décrit dans le présent document a été créé par les contributeurs au groupe de travail OTP de l'IETF. Des contributions spécifiques ont été faites par Neil Haller, qui a fourni des apports pour les exigences de conception globale d'un protocole de réinitialisation, Denis Pinkas, qui a suggéré plusieurs modifications au protocole de réinitialisation proposé à l'origine, et Phil Servita, qui a ouvert le débat sur le premier protocole réel proposé et a fourni des quantités d'apports spécifiques sur la conception et de protocoles et des protocoles antérieurs. Les extensions au défi OTP ont été suggérées par Chris Newman et John Valdes.

Randall Atkinson et Ted T'so ont aussi contribué par leurs idées aux discussions sur les détails des extensions du protocole dans le présent document.

Références

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC1825] R. Atkinson, "Architecture de sécurité pour le protocole Internet", août 1995. *(Obsolète ? voir* RFC2401*)*

[RFC1826] R. Atkinson, "En-tête d'authentification IP", août 1995. *(Obsolète, voir la* RFC2402*)*

[RFC1938] N. Haller, C. Metz, "Système de mot de passe à utilisation unique", mai 1996. (*Obsolète, voir* RFC2289) *(P.S.)*

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

Adresse de l'auteur

Craig Metz
The Inner Net
Box 10314-1936
Blacksburg, VA 24062-0314
(DSN) 354-8590
mél ; cmetz@inner.net

Appendice Réponses de référence

Les réponses suivantes ont été générées par une version de développement d'une mise en œuvre des One-Time Passwords in Everything (OPIE) de la présente spécification.

Toutes sont des réponses au défi : otp-md5 499 ke1234 ext

Noter que les réponses de réinitialisation utilisent la même phrase de passe secrète pour le nouveau et l'actuel et un nouveau germe de "ke1235". Aussi, ces réponses ont été coupées pour les besoins du formatage sur plusieurs lignes ; elles NE DOIVENT PAS être sur plusieurs lignes en utilisation réelle.

La phrase de passe secrète pour ces réponses est : This is a test.

La réponse OTP standard en hexadécimal est :

5bf0 75d9 959d 036f

La réponse OTP standard en six-word est :

BOND FOGY DRAB NE RISE MART

La réponse OTP étendue "hex" est :

hex:5Bf0 75d9 959d 036f

La réponse OTP étendue "word" est :
word:BOND FOGY DRAB NE RISE MART

La réponse OTP étendue "init-hex" est :

init-hex:5bf0 75d9 959d 036f:md5 499 ke1235:3712 dcb4 aa53 16c1

La réponse OTP étendue "init-word" est :

init-word:BOND FOGY DRAB NE RISE MART:md5 499 ke1235: RED HERD NOW BEAN PA BURG

Déclaration complète de droits de reproduction