Groupe de travail Réseau
Request for Comments : 2944
Catégorie : En cours de normalisation

T. Wu, Standford University
septembre 2000
Traduction Claude Brière de L'Isle

Authentification Telnet : SRP

Résumé
Le présent document spécifie un schéma d'authentification pour le protocole Telnet dans le cadre décrit par la [RFC2941], utilisant le mécanisme d'authentification du protocole de mot de passe distant sécurisé (SRP, *Secure Remote Password Protocol*). Le mécanisme spécifique, SRP-SHA1, est décrit dans la [RFC2945].

1. Noms et codes des commandes

Types d'authentification
SRP 5

Commandes de sous-option
AUTH 0
REJECT 1
ACCEPT 2
CHALLENGE 3
RESPONSE 4
EXP 8
PARAMS 9

2. Signification des commandes

IAC SB AUTHENTICATION IS <paire-de-type-d'authentification> AUTH IAC SE

Cette commande indique que le client a fourni le nom d'utilisateur et est prêt à recevoir les paramètres de champ de cet usager. Il n'y a pas d'informations d'authentification à envoyer pour l'instant au côté distant de la connexion. Celles-ci ne devraient être envoyées qu'après que la commande IAC SB AUTHENTICATION NAME a été produite. Si l'octet modificateur (le second octet de la paire de type d'authentification) a des bits autres que AUTH_WHO_MASK ou AUTH_HOW_MASK établis, les deux octets sont inclus dans le hachage de clé de session qui est décrit plus loin. Cela assure une négociation correcte de la paire de type d'authentification, tout en maintenant la rétro compatibilité avec les logiciels existants.

IAC SB AUTHENTICATION REPLY <paire-de-type-d'authentification> PARAMS <valeurs du module, générateur, et sel> IAC SE
Cette commande est utilisée pour passer les trois valeurs de paramètres utilisés dans l'exponentiation chez le client. Ces valeurs sont souvent appelées n, g, et s.

IAC SB AUTHENTICATION IS <paire-de-type-d'authentification> EXP <résidu exponentiel du client> IAC SE
Cette commande est utilisée pour passer le résidu exponentiel du client, appelé aussi A, calculée par rapport aux paramètres échangés précédemment.

IAC SB AUTHENTICATION REPLY <paire-de-type-d'authentification> CHALLENGE <résidu exponentiel du serveur> IAC SE
Cette commande est utilisée pour passer le résidu exponentiel du serveur, calculé par rapport aux mêmes paramètres. Cette quantité est en fait la somme de deux résidus, c'est-à-dire, g^x + g^b. Pour les détails, voir [SRP] et la [RFC2945].

IAC SB AUTHENTICATION IS <paire-de-type-d'authentification> RESPONSE <réponse du client> IAC SE
Cette commande donne au serveur la preuve de l'authenticité du client avec une réponse de 160 bits (20 octets).

IAC SB AUTHENTICATION REPLY <paire-de-type-d'authentification> ACCEPT <réponse du serveur> IAC SE
Cette commande indique que l'authentification a réussi. Le serveur va construire sa propre preuve d'authenticité et l'inclure comme données de sous-option.

IAC SB AUTHENTICATION REPLY <paire-de-type-d'authentification> REJECT <raison facultative de rejet> IAC SE
Cette commande indique que l'authentification a échoué, et si ils y a plus de données dans la sous-option, c'est un message de texte ASCII qui donne la raison du rejet.

Pour la commande PARAMS, comme trois éléments de données sont transmis, chaque paramètre est précédé d'un spécifieur de 16 bits (deux octets) de long, dans l'ordre des octets du réseau. La commande EXP n'a pas de compte devant les données parce qu'il n'y a qu'un seul élément de données dans cette sous-option. Les données de CHALLENGE, RESPONSE, et ACCEPT n'ont elles non plus pas de compte parce qu'elles sont toutes d'une taille fixe.

3. Règles de mise en œuvre

Actuellement, seul le mode AUTH_CLIENT_TO_SERVER est pris en charge. Bien que le protocole SRP effectue effectivement l'authentification mutuelle implicite par suite des preuves bidirectionnelles, seul le mode d'authentification AUTH_HOW_ONE_WAY est actuellement défini. Le réglage AUTH_HOW_MUTUAL est réservé pour une variante d'authentification mutuelle explicite du protocole SRP qui sera définie dans des spécifications futures.

Toutes les données de grands nombres envoyées dans les arguments des commandes PARAMS et EXP doivent être dans l'ordre des octets du réseau, c'est à dire, avec l'octet de poids fort en premier. Aucun bourrage n'est utilisé.

Le mécanisme SRP-SHA1, tel que décrit dans la [RFC2945] génère une clé de session de 40 octets, qui permet aux mises en œuvre d'utiliser des clés différentes pour le trafic entrant et sortant, augmentant la sécurité de la session chiffrée. Il est recommandé que la méthode Telnet ENCRYPT, si elle est utilisée, soit capable de tirer parti de clés de session plus longues.

4. Exemples

L'usager "tjw" peut souhaiter se connecter à une machine "foo". Le client va envoyer IAC SB AUTHENTICATION NAME "tjw" IAC SE IAC SB AUTHENTICATION IS SRP AUTH IAC SE. Le serveur va chercher les paramètres Champ et Sel pour trouver "tjw" dans son fichier des mots de passe et les renvoyer au client. Le client et le serveur vont alors échanger les résidus exponentiels et calculer leurs clés de session (après que le client a rentré "tjw" comme son mot de passe). Puis, le client va envoyer au serveur sa preuve qu'il connaît la clé de session. Le serveur va renvoyer un ACCEPT ou un REJECT. Si le serveur accepte l'authentification, il va aussi envoyer sa propre preuve qu'il connaît la clé de session au client.

Client **Serveur**

IAC DO AUTHENTICATION
IAC WILL AUTHENTICATION

[Le serveur a maintenant toute liberté pour demander les informations d'authentification.]
IAC SB AUTHENTICATION SEND SRP CLIENT|ONE_WAY|
ENCRYPT_USING_TELOPT SRP CLIENT|ONE_WAY IAC SE

[Le serveur a demandé l'authentification SRP. Il a indiqué une préférence pour ENCRYPT_USING_TELOPT, qui exige que l'option Telnet ENCRYPT soit négociée une fois l'authentification réussie. Si le client n'accepte pas cela, le serveur accepte de retomber sur un mode à chiffrement facultatif
Le client va maintenant répondre avec le nom d'utilisateur sous lequel il veut se connecter.]

IAC SB AUTHENTICATION NAME "tjw" IAC SE

IAC SB AUTHENTICATION IS
SRP CLIENT|ONE_WAY|ENCRYPT_USING_TELOPT AUTH IAC SE

[Le serveur cherche "tjw" dans les informations appropriées et renvoie les paramètres dans une commande PARAMS. Les paramètres consistent en les valeurs N, g, et s, chacune étant précédée d'un paramètre d'une taille de deux octets.]

IAC SB AUTHENTICATION REPLY SRP CLIENT|ONE_WAY|
ENCRYPT_USING_TELOPT PARAMS ss ss nn nn nn nn ...
ss ss gg gg gg gg ... ss ss tt tt tt tt ... IAC SE

[Les deux côtés envoient leurs résidus exponentiels. Le client envoie sa valeur A et le serveur envoie sa valeur B. Dans SRP, le message CHALLENGE peut être calculé mais pas envoyé avant la commande EXP.]

IAC SB AUTHENTICATION IS
SRP CLIENT|ONE_WAY|ENCRYPT_USING_TELOPT EXP
aa aa aa aa aa aa aa aa ... IAC SE

IAC SB AUTHENTICATION REPLY SRP CLIENT|ONE_WAY|
ENCRYPT_USING_TELOPT CHALLENGE
bb bb bb bb bb bb bb bb ... IAC SE

[Le client envoie sa réponse au serveur. C'est le message M dans le protocole SRP, qui prouve la possession de la clé de session par le client.
Comme ENCRYPT_USING_TELOPT est spécifié, les deux octets de la paire de type d'authentification sont ajoutés à la clé de session K avant que soit calculé le hachage pour M. Si le client et le serveur se sont mis d'accord sur un mode sans que le fanion Chiffrement soit établi, rien ne sera ajouté à K.
Ce message et la réponse du serveur sont tous deux aussi longs que le résultat du hachage ; la longueur est de 20 octets pour SHA-1.]

IAC SB AUTHENTICATION IS
SRP CLIENT|ONE_WAY|ENCRYPT_USING_TELOPT RESPONSE
xx xx xx xx xx xx xx xx ... IAC SE

[Le serveur accepte la réponse et envoie ses propres preuves.]

IAC SB AUTHENTICATION REPLY SRP CLIENT|ONE_WAY|
ENCRYPT_USING_TELOPT ACCEPT
yy yy yy yy yy yy yy yy ... IAC SE

5. Considérations pour la sécurité

La capacité à négocier un mécanisme d'authentification commun entre client et serveur est une caractéristique de l'option d'authentification qui devrait être utilisée avec prudence. Lorsque la négociation est effectuée, aucune authentification n'est encore survenue. Donc, les deux systèmes n'ont aucun moyen de savoir si ils parlent bien au système prévu. Un intrus pourrait tenter de négocier l'utilisation d'un système d'authentification qui serait faible, ou déjà compromis par l'intrus.

Comme SRP s'appuie sur la sécurité du système de chiffrement à clé publique sous-jacent, le modulo "n" devrait être assez grand pour résister à une attaque en force brute. Une longueur d'au moins 1024 bits est recommandée, et les mises en œuvre devraient rejeter les tentatives d'utiliser des modulos qui font moins de 512 bits, ou les tentatives d'utiliser des modulos et paramètres générateurs invalides (un "n" premier non sûr ou un "g" non primitif).

6. Considerations relatives à l'IANA

Le type d'authentification SRP et ses valeurs de sous-options associées sont enregistrés auprès de l'IANA. Toutes les valeurs de sous-option utilisées pour étendre le protocole décrit dans le présent document doivent être enregistrées auprès de l'IANA avant utilisation. L'IANA a reçu pour instruction de ne pas donner de nouvelles valeurs de sous-option sans que soit soumise la documentation de leur utilisation.

7. Références

[RFC2941] T. Ts'o, éd., J. Altman, "Option d'authentification Telnet", septembre 2000. *(P.S.)*

[SRP] T. Wu, "The Secure Remote Password Protocol", In Proceedings of the 1998 ISOC Network and Distributed System Security Symposium, San Diego, CA, pp. 97-111.

[RFC2945] T. Wu, "Système SRP d'authentification et d'échange de clés", septembre 2000. *(P.S.)*

8. Adresse de l'auteur

Thomas Wu
Stanford University
Stanford, CA 94305
mél : tjw@cs.Stanford.EDU

9. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuellement assuré par la Internet Society.