Groupe de travail Réseau
Request for Comments : 2942
Catégorie : En cours de normalisation

T. Ts'o, VA Linux Systems
septembre 2000
Traduction Claude Brière de L'Isle

Authentification Telnet : Kerberos version 5

Résumé
Le présent document décrit comment Kerberos version 5 [RFC1510] est utilisé avec le protocole Telnet. Il décrit une sous option d'authentification Telnet à utiliser avec l'option d'authentification Telnet [RFC2941]. Ce mécanisme peut aussi être utilisé pour fournir le matériel de clés pour les services de confidentialité des données en conjonction avec l'option de chiffrement Telnet [RFC2946].

1. Noms et codes des commandes

Types d'authentification : KERBEROS_V5 2

Commandes de sous option :

AUTH	0
REJECT	1
ACCEPT	2
RESPONSE	3
FORWARD	4
FORWARD_ACCEPT	5
FORWARD_REJECT	6

2. Signification des commandes

IAC SB AUTHENTICATION IS <paire de type d'authentification> AUTH <message KRB_AP_REQ Kerberos v5> IAC SE
Ceci est utilisé pour passer le message KRB_AP_REQ de Kerberos V5 [RFC1510] au côté distant de la connexion. Le premier octet de la valeur de <paire de type d'authentification> est KERBEROS_V5, pour indiquer que la version 5 de Kerberos est utilisée. L'authentifiant Kerberos V5 dans le message KRB_AP_REQ doit contenir une somme de contrôle Kerberos V5 de la paire de types d'authentification de deux octets. Cette somme de contrôle doit être vérifiée par le serveur pour s'assurer que la paire de types d'authentification a été correctement négociée. L'authentifiant Kerberos V5 doit aussi comporter le champ facultatif de sous-clé, qui devra être rempli avec une clé choisie de façon aléatoire. Cette clé devra être utilisée pour les besoins du chiffrement si le chiffrement est négocié, et elle devra être utilisée comme clé de session négociée (c'est-à-dire utilisée comme keyid 0) pour les besoins de l'option de chiffrement Telnet ; si le champ sous-clé n'est pas rempli, la clé de ticket de session sera utilisée à la place.

Si des services de confidentialité des données sont désirés, le fanion ENCRYPT_US-ING_TELOPT doit être établi dans la paire de types d'authentification comme spécifié dans la [RFC2941].

IAC SB AUTHENTICATION REPLY <paire de type d'authentification> ACCEPT IAC SE
Cette commande indique que l'authentification a réussi.
Si le bit AUTH_HOW_MUTUAL est établi dans le second octet de la paire type d'authentification, la commande RESPONSE doit être envoyée avant l'envoi de la commande ACCEPT.

IAC SB AUTHENTICATION REPLY <paire de type d'authentification> REJECT <cause facultative du rejet> IAC SE
Cette commande indique que l'authentification n'a pas réussi, et si il y a des données en plus dans la sous option, c'est un message de texte ASCII disant la raison du rejet.

IAC SB AUTHENTICATION REPLY <paire de type d'authentification> RESPONSE <message KRB_AP_REP> IAC SE
Cette commande est utilisée pour effectuer l'authentification mutuelle. Elle n'est utilisée que lorsque le bit AUTH_HOW_MUTUAL est établi dans le second octet de la paire de type d'authentification. Après la vérification d'une commande AUTH, une commande RESPONSE est envoyée contenant un message Kerberos V5 KRB_AP_REP pour effectuer l'authentification mutuelle.

IAC SB AUTHENTICATION <paire de type d'authentification> FORWARD <message KRB_CRED> IAC SE
Cette commande est utilisée pour transmettre des accréditifs Kerberos à l'usage de la session distante. Les accréditifs sont passés comme un message KRB_CRED de Kerberos V5 qui comporte entre autres choses le ticket Kerberos transmis et une clé de session associée au ticket. Une partie du message KRB_CRED est chiffrée avec la clé précédemment échangée pour la session Telnet par la sous option AUTH.

IAC SB AUTHENTICATION <paire de type d'authentification> FORWARD_ACCEPT IAC SE
Cette commande indique que la transmission des accréditifs a réussi.

IAC SB AUTHENTICATION <paire de type d'authentification> FORWARD_REJECT <cause facultative du rejet> IAC SE
Cette commande indique que la transmission des accréditifs n'a pas réussi, et si il y a plus de données dans la sous option, c'est un message texte en ASCII de la cause du rejet.

3. Règles de mise en œuvre

Si le second octet de la paire de type d'authentification a le bit AUTH_WHO réglé à AUTH_CLIENT_TO_SERVER, le client envoie alors la commande AUTH initiale, et le serveur répond soit pas ACCEPT soit par REJECT. De plus, si le bit AUTH_HOW est réglé à AUTH_HOW_MUTUAL, le serveur enverra une RESPONSE avant d'envoyer le ACCEPT.

Si le second octet de la paire de type d'authentification a le bit AUTH_WHO réglé à AUTH_SERVER_TO_CLIENT, le serveur envoie alors la commande AUTH initiale, et le client répond soit par ACCEPT soit par REJECT. De plus, si le bit AUTH_HOW est réglé à AUTH_HOW_MUTUAL, le client enverra une RESPONSE avant d'envoyer le ACCEPT.

Le principal Kerberos utilisé par le serveur va généralement être de la forme "hôte/<nom-d'hôte>@domaine". C'est-à-dire que le premier composant du principal Kerberos est "hôte" ; le second composant est le nom d'hôte pleinement qualifié en minuscules du serveur ; et le domaine est le domaine Kerberos auquel appartient le serveur.

Tout caractère Telnet IAC qui survient dans les messages KRB_AP_REQ ou KRB_AP_REP, dans la structure KRB_CRED, ou dans la chaîne facultative de texte de rejet doit être doublé comme spécifié dans la [RFC0855]. Autrement l'octet suivant risquerait d'être pris pour une commande Telnet.

4. Exemples

L'utilisateur "joe" souhaite se connecter comme étant l'utilisateur "pete" sur la machine "foo". Si "pete" a réglé les choses sur "foo" pour permettre à "joe" d'accéder à son compte, le client va alors envoyer :

IAC SB AUTHENTICATION NAME "pete" IAC SE IAC SB AUTHENTICATION IS KERBEROS_V5 AUTH <KRB_AP_REQ_MESSAGE> IAC SE

Le serveur va alors authentifier l'usager comme "joe" à partir du KRB_AP_REQ_MESSAGE, et si le KRB_AP_REQ_MESSAGE est accepté par Kerberos, et si "pete" a permis à "joe" d'utiliser son compte, le serveur va alors continuer la séquence d'authentification en envoyant une RESPONSE (pour faire l'authentification mutuelle, si elle est demandée) suivie par le ACCEPT.

Si la transmission en a été demandée, le client envoie alors IAC SB AUTHENTICATION IS KERBEROS_V5 CLIENT| MUTUAL FORWARD < structure KRB_CRED avec les accréditifs à transmettre> IAC SE. Si le serveur réussit à lire les accréditifs transmis, il envoie alors FORWARD_ACCEPT, autrement, c'est un FORWARD_REJECT qui est renvoyé.

Client **Serveur**

IAC WILL AUTHENTICATION IAC DO AUTHENTICATION

[Le serveur est maintenant libre pour demander les informations d'authentification.]

IAC SB AUTHENTICATION SEND
KERBEROS_V5 CLIENT|MUTUAL
KERBEROS_V5 CLIENT|ONE_WAY IAC SE

[Le serveur a demandé l'authentification mutuelle Kerberos version 5. Si l'authentification mutuelle n'est pas acceptée, le serveur veut alors faire une authentification unidirectionnelle. Le client va maintenant répondre avec le nom d'utilisateur sous lequel il veut se connecter, et le ticket Kerberos.]

IAC SB AUTHENTICATION NAME "pete" IAC SE
IAC SB AUTHENTICATION IS KERBEROS_V5 CLIENT|
MUTUAL AUTH <message KRB_AP_REQ> IAC SE

[Comme l'authentification mutuelle est désirée, le serveur envoie une RESPONSE pour prouver qu'il est réellement le bon serveur.]

IAC SB AUTHENTICATION REPLY
KERBEROS_V5 CLIENT|MUTUAL
RESPONSE <message KRB_AP_REP> IAC SE

[Le serveur répond par une commande ACCEPT pour déclarer que l'authentification a réussi.]

IAC SB AUTHENTICATION REPLY
KERBEROS_V5 CLIENT|MUTUAL ACCEPT IAC SE

[Si c'est demandé, le client envoie maintenant la commande FORWARD pour transmettre les accréditifs au site distant.]

IAC SB AUTHENTICATION IS KER-
BEROS_V5 CLIENT|MUTUAL
FORWARD <message KRB_CRED> IAC SE

[Le serveur répond par une commande FORWARD_ACCEPT pour déclarer que la transmission des accréditifs a réussi.]

IAC SB AUTHENTICATION REPLY
KERBEROS_V5 CLIENT|MUTUAL
FORWARD_ACCEPT IAC SE

5. Considérations pour la sécurité

Le choix d'une clé de session aléatoire dans l'authentifiant Kerberos V5 est critique, car cette clé sera utilisée pour chiffrer le flux de données Telnet si le chiffrement est activé. Il est fortement recommandé que le choix de la clé aléatoire soit fait en utilisant les techniques cryptographiques qui impliquent la clé de session du ticket Kerberos. Par exemple, utiliser l'heure en cours, la chiffrer avec la clé de session du ticket, puis corriger la parité de la clé est une façon forte de générer une clé de sous session, car la clé de session du ticket est supposée n'être jamais divulguée à un attaquant.

Il faudrait faire attention avant de transmettre les accréditifs Kerberos d'un usager au serveur distant. Si le serveur distant n'est pas digne de confiance, il pourrait en résulter la compromission des accréditifs de l'usager. Donc, l'interface d'utilisateur ne devrait pas transmettre par défaut les accréditifs ; il serait bien plus sûr d'exiger que l'usager demande explicitement la transmission des accréditifs pour chaque connexion, ou d'avoir une liste d'hôtes de confiance pour lesquels la transmission des accréditifs est activée, mais de ne pas activer la transmission des accréditifs par défaut pour toutes les machines.

Le message IAC SB AUTHENTICATION NAME nom IAC SE n'est pas protégé dans ce protocole. Son contenu devrait être vérifié par une méthode sûre après la fin de l'authentification avant qu'il soit utilisé.

6. Considérations relatives à l'IANA

Le type d'authentification KERBEROS_V5 et ses valeurs de sous option associées sont enregistrés auprès de l'IANA. Toutes les valeurs de sous option utilisées pour étendre le protocole tel que 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 la soumission de la documentation de leur usage.

7. Remerciements

Le présent document a été à l'origine écrit par Dave Borman de Cray Research, Inc. Theodore Ts'o du MIT l'a revu pour qu'il reflète les derniers apports de l'expérience. Cliff Neuman et Prasad Upasani de l'Institut des sciences de l'information de USC ont développé le support de transmission des accréditifs.

De plus, les membres du groupe de travail Telnet sont chaleureusement remerciés de leurs contributions.

8. Références

[RFC0855] J. Postel et J. Reynolds,"Spécifications des options TELNET", mai 1983.

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir RFC4120)*

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

[RFC2946] T. Ts'o, "Option Telnet de chiffrement des données", septembre 2000. *(P.S.)*

9. Adresse de l'éditeur

Theodore Ts'o
VA Linux Systems
43 Pleasant St.
Medford, MA 02155
USA
téléphone : (781) 391-3464
mél : tytso@mit.edu

10. Déclaration complète de droits de reproduction

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