

Groupe de travail Réseau
Request for Comments : 4537
RFC mise à jour : 4120
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

L. Zhu, P. Leach, K. Jaganathan
Microsoft Corporation
juin 2006

Extension de négociation du système cryptographique Kerberos

Statut de ce mémoire

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

Notice de Copyright

Copyright (C) The Internet Society (2006).

Résumé

Le présent document spécifie une extension au protocole Kerberos défini dans la RFC 4120, dans laquelle le client peut envoyer une liste des types de chiffrement acceptés en ordre de préférence décroissante, et le serveur peut choisir un type de chiffrement qui soit accepté à la fois par le client et le serveur.

1 Introduction

Avec le mécanisme actuel de la [RFC4120], le Centre de distribution Kerberos (KDC) doit limiter le type de chiffrement de clé de session de ticket (enctype) choisi pour un serveur donné à un type qu'il suppose accepté à la fois par le client et le serveur. Si le client et le serveur comprennent tous deux un enctype plus fort que celui choisi par le KDC, il ne peuvent pas le négocier. Il en résulte que la protection du trafic d'application est souvent plus faible qu'il n'est nécessaire lorsque le serveur peut prendre en charge des ensembles différents de enctype selon le logiciel d'application du serveur utilisé.

Le présent document spécifie une extension au protocole Kerberos pour permettre aux clients et aux serveurs de négocier l'utilisation d'un système de chiffrement différent et éventuellement plus fort dans la communication ultérieure.

Cette extension utilise un élément de donnée d'autorisation dans l'authentifiant du message AP-REQ de la [RFC4120]. Le client envoie la liste des enctype qu'il accepte au serveur ; le serveur informe alors le client de son choix. La sous clé négociée est envoyée dans le message AP-REP de la [RFC4120].

2 Conventions utilisées dans le présent document

Dans le présent document, les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14 [RFC2119].

3 Extension de négociation

Si le client préfère un entype à celui de la clé de session de ticket du service, il DEVRAIT alors envoyer une liste des entype en ordre de préférence décroissante au serveur. Sur la base d'une politique locale, le client choisira les entype parmi les entype disponibles localement pour les inclure dans cette liste, et il NE DEVRAIT PAS inclure d'entype qui ait une préférence moindre que celle de la clé de session de ticket dans le ticket de service ticket. De plus, le client NE DEVRAIT PAS inclure de numéros d'entype négatifs (utilisation locale) à moins qu'il ne sache a priori que le serveur a été configuré pour utiliser les mêmes numéros négatifs d'entype pour les mêmes entype.

Le client envoie la liste d'entype via les données d'autorisation de l'authentifiant dans la AP-REQ [RFC4120]. Un nouveau type d'élément de données d'autorisation AD-ETYPE-NEGOTIATION est défini.

AD-ETYPE-NEGOTIATION 129

Cet élément de données d'autorisation est inclus dans le conteneur AD-IF-RELEVANT ; et donc, un serveur correctement mis en œuvre qui ne comprend pas cet élément devrait l'ignorer [RFC4120]. La valeur de cet élément d'autorisation contient le codage DER [X680] [X690] des types ASN.1 suivants :

```
EtypeList ::= SEQUENCE OF Int32
    -- Spécifie les entype acceptés par le client.
    -- Cette liste d'entype est en ordre de préférence décroissant (le favori en premier).
    -- Int32 est défini dans la [RFC4120].
```

Si la EtypeList est présente et si le serveur préfère un entype provenant de la liste de entype du client à celui de la sous clé de l'authentifiant AP-REQ (si il est présent) ou à la clé de session du ticket de service, le serveur DOIT créer une sous clé utilisant cet entype. Cette sous clé négociée est envoyée dans le champ sous clé du message AP-REP, et elle est alors utilisée comme clé du protocole ou clé de base [RFC3961] de la communication ultérieure.

Si le entype de la clé de session de ticket est incluse dans la liste des entype envoyée par le client, il DEVRAIT être le dernier de la liste ; autrement, cet entype NE DOIT PAS être négocié s'il n'était pas inclus dans la liste.

Cette extension de négociation NE DEVRAIT PAS être utilisée lorsque le client n'attend pas de sous clé dans le message AP-REP provenant du serveur.

Note sur la génération de clés : Le KDC a un fort générateur de nombres pseudo aléatoires (PRNG, *Pseudo-Random Number Generator*) ; comme tel, le client peut tirer parti du caractère aléatoire fourni par le KDC en réutilisant les données de clé du KDC lors de la génération des clés. Les mises en oeuvre DEVRAIENT utiliser la valeur de clé de session de ticket de service comme source supplémentaire d'entropie lors de la génération des sous clés négociées. Si la sous clé d'authentifiant AP-REQ est présente, elle PEUT aussi être utilisée comme source d'entropie.

Le serveur PEUT ignorer l'ordre de préférence indiqué par le client. La politique par laquelle le client ou le serveur choisit un entype (c'est-à-dire, comment est choisi l'ordre de préférence pour les entype choisis) est une affaire locale.

4 Considérations pour la sécurité

La liste entype du client et la réponse entype du serveur font partie des données chiffrées, et donc, les considérations pour la sécurité sont les mêmes que celles des données chiffrées de Kerberos.

La liste EtypeList et la clé de sous session du serveur sont toutes deux protégées par la clé de session ou la clé de sous-session utilisée pour AP-REQ, et il en résulte que, si une clé pour un entype plus fort est négociée au dessous d'une clé pour un entype plus faible, un attaquant capable de briser l'entype plus faible peut aussi découvrir la clé pour l'entype plus fort. L'avantage de cette extension est de minimiser la quantité de texte chiffré encrypté sous un entype plus faible auquel un attaquant a accès.

5 Remerciements

Les auteurs remercient chaleureusement les personnalités suivantes pour leurs commentaires et suggestions : Ken Raeburn, Luke Howard, Tom Yu, Love Hornquist Astrand, Sam Hartman, et Martin Rex.

6 Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC3961] K. Raeburn, "Spécifications de chiffrement et de somme de contrôle pour Kerberos 5", février 2005.
- [RFC4120] C. Neuman et autres, "[Service Kerberos d'authentification de réseau](#) (V5)", juillet 2005. (*MàJ par RFC4537, RFC5021*)
- [X.680] Union Internationale des Télécommunications - Secteur de la Normalisation des Télécommunications, "Notation numéro un de syntaxe abstraite (ASN.1) - Spécification de la notation de base", X.680 (1997) (aussi ISO/CEI 8824-1:1998).
- [X.690] Union Internationale des Télécommunications - Secteur de la Normalisation des Télécommunications, "Spécification des règles de codage ASN.1 : Règles de codage de base (BER), Règles de codage canonique (CER), et Règles de codage distinctives (DER)", X.690 (1997) (aussi ISO/CEI 8825-1:1998).

Adresse des auteurs

Larry Zhu	Paul Leach	Karthik Jaganathan
Microsoft Corporation	Microsoft Corporation	Microsoft Corporation
One Microsoft Way	One Microsoft Way	One Microsoft Way
Redmond, WA 98052	Redmond, WA 98052	Redmond, WA 98052
USA	USA	USA
mél : lzhu@microsoft.com	mél : paulle@microsoft.com	mél : karthikj@microsoft.com

Déclaration de copyright

Copyright (C) The Internet Society (2006).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et LE CONTRIBUTEUR, L'ORGANISATION QU'IL OU ELLE REPRÉSENTE OU QUI LE/LA FINANCE (S'IL EN EST) LA INTERNET SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI-ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79. Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>. L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est fourni par la Administrative Support Activity (IASA) de l'IETF.