Groupe de travail Réseau
Request for Comments : 5554
RFC mise à jour : 2743
Catégorie : Sur la voie de la normalisation

N. Williams, Sun
mai 2009

Traduction Claude Brière de L'Isle

Précisions et extensions à l'Interface générique de programme d'application de service de sécurité (GSS-API) pour l'utilisation de liens de canal

Résumé
Le présent document précise et généralise la facilité de "liens de canal" de l'interface générique de programmation d'application de service de sécurité (GSS-API, *Generic Security Service Application Programming Interface*), et impose des exigences aux futurs mécanismes GSS-API et de liens de langage de programmation de GSS-API.

Table des matières

1. Introduction....1
2. Conventions utilisées dans ce document....1
3. Nouvelles exigences pour les mécanismes GSS-API....2
4. Structure générique pour les liens de canal GSS-API....2
5. Considérations sur la sécurité....2
6. Références....3
6.1 Références normatives....3
6.2 Références pour information....3
Adresse de l'auteur....3

1. Introduction

La spécification de base de GSS-API version 2, mise à jour 1 de la [RFC2743], fournit une facilité pour le lien de canal (voir aussi la [RFC5056]), mais son traitement est incomplet. La spécification de liens C- de GSS-API [RFC2744] s'étend un peu sur cette facilité en cequ'elle devrait être un moyen générique, mais est en fait une façon spécifique de C-, laissant donc incomplet le traitement de cette facilité.

Le présent document précise la facilité de lien de canal GSS-API et généralise ses parties qui sont spécifiées dans le document de liens C- mais qui devraient avoir été génériques depuis le début.

2. Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le

BCP 14, [RFC2119].

3. Nouvelles exigences pour les mécanismes GSS-API

Étant donnée la publication de la RFC 5056, on affirme maintenant que tous les nouveaux mécanismes GSS-API qui prennent en charge le lien de canal DOIVENT se conformer à la [RFC5056].

4. Structure générique pour les liens de canal GSS-API

La spécification de base de la version 2 de GSS-API 2, mise à jour 1 [RFC2743] fournit une facilité pour le lien de canal. Elle modélise les liens de canal comme une "OCTET STRING" *(chaîne d'octets)* et laisse à la spécification de liens C- de GSS-API version 2, mise à jour 1, de spécifier la structure des chaînes d'octets du contenu des liens de canal. La spécification de liens C- [RFC2744] définit alors, en termes de C, ce qui devrait avoir été une structure générique pour les liens de canal. Le mécanisme GSS Kerberos V [RFC4121] définit aussi une méthode pour coder les liens de canal GSS d'une façon indépendante des liens C- -- autrement, la facilité de lien de canal du mécanisme ne serait pas utilisable avec d'autres liens de langage.

En d'autres termes, la structure des liens de canal GSS donnée dans la [RFC2744] est en fait générique en dépit d'être spécifiée en termes de concepts et syntaxe C.

On la généralise comme montré ci-dessous, en utilisant le même pseudo ASN.1 qu'utilisé dans la RFC 2743. Bien que la figure ci-dessous soit, bien sûr, un type d'ASN.1 valide [X.680], on ne fournit pas un module ASN.1 complet car il n'est pas nécessaire parce que aucun codage standard de cette structure n'est nécessaire -- la définition ci-dessous fait partie d'une API abstraite, aucune partie d'un protocole ne définissant de bits sur le réseau. Les mécanismes GSS-API n'ont pas besoin de coder le contenu de cette structure, mais ce codage va être spécifique du mécanisme (voir ci-dessous).

```
GSS-CHANNEL-BINDINGS ::= SEQUENCE {
        initiator-address-type  INTEGER,        -- voir la RFC2744
        initiator-address       OCTET STRING,   -- voir la RFC2744
        acceptor-address-type   INTEGER,        -- voir la RFC2744
        acceptor-address        OCTET STRING,   -- voir la RFC2744
        application-data        OCTET STRING,   -- voir la RFC5056
  }
```

Structure abstraite de liens de canal GSS-API

Les valeurs des champs d'adresse sont décrites dans la [RFC2744].

Les nouveaux liens spécifiques de langage de GSS-API DEVRAIENT spécifier une formulation spécifique du langage de cette structure.

Lorsque un lien de langage de la GSS-API modélise les liens de canal comme des OCTET STRING (ou l''équivalent dans le langage) alors la mise en œuvre DOIT supposer que ces liens correspondent seulement au champ Données d'application des GSS-CHANNEL-BINDINGS comme montré ci dessus, plutôt qu'à un codage de GSS-CHANNEL-BINDINGS.

Comme mentionné ci-dessus, la [RFC4121] décrit un codage de la structure GSS-CHANNEL-BINDINGS et ensuite hache ce codage. Les autres mécanismes GSS-API sont libres d'utiliser ce codage.

5. Considérations sur la sécurité

Pour les considérations générales de sécurité relatives aux liens de canal, voir la [RFC5056].

Les liens de langage qui utilisent OCTET STRING (ou son équivalent) pour les liens de canal ne vont pas prendre en charge l'utilisation d'adresses réseau comme liens de canal. Cela ne devrait pas causer de problème de sécurité, car l'utilisation d'adresses réseau comme liens de canal n'est généralement pas sûre. Cependant, il est important que "les liens

de canal de point d'extrémité" ne soient pas modélisés comme des adresses réseau ; autrement, ces liens de canal ne peuvent pas être utilisables avec tous les liens de langage dans la GSS-API.

6. Références

6.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC2743] J. Linn, "Interface générique de programme d'application de service de sécurité, version 2, mise à jour 1", janvier 2000. (*MàJ par* RFC5554)

[RFC2744] J. Wray, "API de service générique de sécurité, version 2 : liaisons C", janvier 2000. *(P.S.)*

[RFC4121] L. Zhu et autres, "Version 2 du mécanisme d'interface de programme d'application de service de sécurité générique (GSS-API) de Kerberos version 5", juillet 2005. (*MàJ* RFC1964) (*MàJ par les* RFC6542, 6649, 8062)) *(P.S.)*

[RFC5056] N. Williams, "Sur l'utilisation des liaisons de canaux pour sécuriser les canaux", novembre 2007. *(P.S.)*

6.2 Références pour information

[X.680] Recommandation UIT-T X.680 | ISO/CEI 8824-1:2002 "Technologies de l'information - Notation de syntaxe abstraite n°1 (ASN.1) : Spécification de la notation de base". (07/2002)

Adresse de l'auteur

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
US
mél : Nicolas.Williams@sun.com