Groupe de travail Réseau
Request for Comments : 5178
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

N. Williams, Sun
A. Melnikov, Isode Ltd.
mai 2008

Internationalisation des noms de service fondés sur le domaine et type de nom d'interface de programme d'application de service générique de sécurité (GSS-API)

Résumé
Le présent document décrit les noms principaux de service fondés sur le nom de domaine et le type de nom correspondant pour l'interface de programme d'application de service générique de sécurité (GSS-API, *Generic Security Service Application Programming Interface*). L'internationalisation de la GSS-API est aussi traitée.

Les noms de service fondés sur le domaine sont similaires aux noms de service fondés sur l'hôte, mais en utilisant un nom de domaine (pas nécessairement un nom de domaine Internet) en plus d'un nom d'hôte. Le principal objet des noms fondés sur le domaine est de fournir une mesure de protection aux applications qui utilisent des protocoles de découverte de service non sûrs. Ceci est fait en fournissant un moyen de désigner des services en grappes d'après le "domaine" qu'ils desservent, permettant ainsi à leurs clients d'autoriser les serveurs du service sur la base de l'authentification de leurs noms de service.

Table des Matières

1. Introduction

Certaines applications ont besoin de découvrir les noms des serveurs pour une ressource spécifique. Certaines méthodes courantes pour la découverte de serveur ne sont pas sûres, par exemple, les interrogations au DNS [RFC1035] sur les enregistrements de ressources SRV [RFC2782] sans utiliser DNSSEC [RFC4033], et sont sujettes à des attaques par lesquelles un client peut être redirigé sur un serveur incorrect et éventuellement malveillant. Un client peut même être redirigé sur un serveur qui a des accréditifs pour lui-même et peut donc s'authentifier auprès du client, et pourrait être incorrect ou malveillant (disons, parce qu'il a été compromis).

Les noms fondés sur le domaine permettent aux applications initiatrices de GSS-API [RFC2743] (clients) d'autoriser des principaux acceptants (serveurs) à servir la ressource pour laquelle le client a utilisé une découverte non sûre de serveur sans sécuriser la méthode de découverte de serveur ni exiger un protocole supplémentaire pour l'autorisation du serveur. C'est-à-dire, soit un serveur découvert a des accréditifs pour authentifier les noms de service fondés sur le domaine auquel il est prévu de répondre, soit il n'en a pas. La disponibilité d'accréditifs valides pour authentifier les noms fondés sur le domaine implique l'autorisation d'un serveur donné sur un service à l'échelle du domaine.

Un nom fondé sur le domaine consiste en trois éléments exigés :
o un nom de service
o un nom de domaine
o un nom d'hôte

Le nom de domaine et le nom d'hôte devraient être des noms du système des noms de domaine (DNS, *Domain Name System*) bien que les noms fondés sur le domaine pourraient être utilisés dans des environnements non DNS. À cause de l'utilisation des noms DNS, on doit aussi assurer l'internationalisation de la GSS-API.

Noter que la désignation fondée sur le domaine n'est pas nouvelle. Selon un rapport à la liste de diffusion du groupe de travail KITTEN, il existe au moins une mise en œuvre de LDAP qui utilise la désignation de service fondée sur le domaine, et le mécanisme DIGEST-MD5 HTTP/authentification simple et couche de sécurité (SASL) [RFC2831] décrit une notion similaire. (Voir au paragraphe 2.1.2 de la [RFC2831] une description du champ "serv-name" de la réponse de résumé.)

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. Considérations relatives à l'IANA

3.1 OID de type de nom

L'IANA a enregistré le nouvel OID de type de nom suivant dans le registre "SMI Security for Name System Designators Codes (nametypes)" *(Sécurité de SMI pour les codes de désignation de système de noms)* :

5 : gss-domain-based-services [RFC5178]

3.2 OID de type de nom et nom symbolique

Le présent document crée un nouveau type de nom GSS-API, avec un nom symbolique de "GSS_C_NT_DOMAINBASED_SERVICE" et cet OID :

{iso(1) org(3) dod(6) internet(1) security(5) nametypes(6) gss-domain-based(5)}

4. Syntaxes d'interrogation et d'affichage

Il y a une seule syntaxe de nom pour les noms fondés sur le domaine. Elle est exprimée en utilisant l'ABNF [RFC5234].

La syntaxe est :
domain-based-name = service "@" domain "@" hostname
hostname = domain
domain = sub-domain 1*("." sub-domain)
sub-domain = Let-dig [Ldh-str]
Let-dig = ALPHA / DIGIT
Ldh-str = *(ALPHA / DIGIT / "-") Let-dig

Où <service> est défini au paragraphe 4.1 de la [RFC2743]. Les autres règles non définies ci-dessus sont définies à l'Appendice B.1 de la [RFC5234].

4.1 Exemples de noms fondés sur le domaine

Ces exemples ne sont pas normatifs :
o ldap@somecompany.exemple@ds1.somecompany.exemple
o nfs@somecompany.exemple@nfsroot1.somecompany.exemple

Le domaine de niveau supérieur .exemple est utilisé ici conformément à la [RFC2606].

5. Considérations d'internationalisation (I18N)

On introduit de nouvelles versions de GSS_Import_name() et de GSS_Display_name() pour mieux prendre en charge Unicode. De plus, on assure l'utilisation du DNS en codage compatible ASCII (ACE, *ASCII Compatible Encoding*) dans les interfaces non internationalisées [RFC3490].

5.1 Importation de noms internationalisés

Quand le paramètre input_name_type est GSS_C_NT_DOMAINBASED_SERVICE OID, alors les mises en œuvre de GSS_Import_name() et les mécanismes GSS-API DOIVENT accepter les noms de domaine codés en ACE internationalisés dans les créneaux nom d'hôte et nom de domaine de la chaîne de nom fondée sun le domaine.

La prise en charge de noms de domaine internationalisés non ASCII DEVRAIT aussi être fournie par une nouvelle fonction, GSS_Import_name_utf8() qui opère exactement comme GSS_Import_name() (avec les mêmes paramètres d'entrée et de sortie et comportement) sauf qu'elle DOIT accepter les noms de domaine internationalisés comme des chaînes UTF-8 et comme des chaînes codées en ACE via son argument input_name_string.

5.2 Affichage de noms internationalisés

Les mises en œuvre de GSS_Display_name() DOIVENT seulement avoir en sortie des noms de domaine internationalisés en US-ASCII ou en codage ACE dans les créneaux de nom d'hôte et de nom de domaine des noms fondés sur le domaine (ou noms de mécanisme qui se conforment à la forme du mécanisme pour les noms fondés sur le domaine).

La prise en charge de noms de domaine internationalisés non ASCII DEVRAIT aussi être fournie par une nouvelle fonction, GSS_Display_name_utf8() qui opère exactement comme GSS_Display_name() (avec les mêmes paramètres d'entrée et de sortie et comportement) sauf qu'elle sort des chaînes UTF-8 via son argument de sortie name_string. GSS_Display_name_utf8() NE DOIT PAS sortir des noms de domaine internationalisés codés en ACE.

6. Exemples de protocole d'application

Les exemples qui suivent ne sont pas normatifs. Ils décrivent comment les auteurs envisagent l'utilisation des noms fondés sur le domaine de deux applications.

6.1 Découverte de serveur racine d'espace de noms NFSv4 à l'échelle du domaine

Un travail est en cours pour fournir une méthode pour construire des espaces de noms de systèmes de fichiers NFSv4 [RFC3530] à l'échelle du domaine où il y a une seule "racine" avec un ou plusieurs serveurs (répliques) et plusieurs systèmes de fichiers collés dans l'espace de noms par l'utilisation de "référants". Les clients pourraient alors construire un espace de noms "global" en utilisant la hiérarchie de domaines du DNS.

Ici, les clients vont toujours savoir, d'après le contexte, quand ils ont besoin de trouver les serveurs racines pour un certain domaine du DNS. La découverte du serveur racine va être effectuée en utilisant les recherches de RR SRV du DNS, sans utiliser le DNSSEC lorsque DNSSEC n'a pas été déployé.

Quand on utilise RPCSEC_GSS [RFC2203] pour la sécurité, les clients NFSv4 vont utiliser des noms fondés sur le domaine pour s'assurer que les serveurs désignés dans les RR SRV sont en fait autorisés à être les serveurs racines NFSv4 pour le domaine cible.

6.2 Découverte de serveur LDAP

Les clients LDAP qui utilisent GSS-API à travers SASL vont aussi bénéficier de l'utilisation des noms fondés sur le domaine pour protéger la découverte de serveur à travers des recherches de RR SRV non sûres du DNS, un peu comme décrit ci-dessus.

À la différence des clients NFSv4, tous les clients LDAP ne savent pas toujours d'après le contexte quand ils devraient utiliser des noms fondés sur le domaine. C'est parce que les clients existants peuvent utiliser une désignation fondée sur l'hôte pour authentifier les serveurs découverts par des recherches de RR SRV. Faire changer ces clients pour qu'ils utilisent une désignation fondée sur le domaine quand des accréditifs d'acceptation fondés sur le domaine n'ont pas été déployés sur les serveurs LDAP, ou quand les serveurs LDAP n'ont pas été modifiés pour permettre l'utilisation de désignations fondées sur le domaine, casserait l'interopérabilité. C'est-à-dire qu'il y a ici un problème d'interopérabilité avec les serveurs traditionnels. Donc, les clients LDAP peuvent devoir faire de la configuration supplémentaire au moment du déploiement pour activer (ou désactiver) l'utilisation de la désignation fondée sur le domaine.

Note : que SASL [RFC4422] ou ses ponts GSS-API [RFC4752], [RFC5801] exigent des mises à jour pour permettre l'utilisation de noms fondés sur le domaine n'est pas pertinent pour la théorie de comment la désignation fondée sur le domaine va protéger la découverte de serveur des clients LDAP.

7. Considérations sur la sécurité

L'utilisation de noms fondés sur le domaine par GSS-API peut n'être pas négociable par certains mécanismes GSS-API, et certains acceptants peuvent ne pas prendre en charge les noms fondés sur le domaine de GSS-API. Dans ce cas, les initiateurs vont devoir se replier sur l'utilisation de noms fondés sur l'hôte, de sorte que les initiateurs DOIVENT aussi vérifier que le nom fondé sur l'hôte de l'acceptant est autorisé à fournir le service concerné pour le domaine que voulait l'initiateur.

Le problème de sécurité ci-dessus s'applique aussi à tous les initiateurs GSS-API qui ne prennent pas en charge les noms de service fondés sur le domaine.

Noter que, comme avec tous les noms de service, la simple existence d'un nom de service fondé sur le domaine porte des informations significatives qui peuvent être utilisées par les initiateurs pour prendre des décisions d'autorisation ; donc, les administrateurs de services d'authentfication répartis devraient avoir conscience de la signification des noms de service pour lesquels ils créent des accréditifs d'acceptation.

8. Références

8.1 Références normatives

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

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

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

[RFC2831] P. Leach et C. Newman, "Utilisation de l'authentification par résumé comme mécanisme SASL", mai 2000. (*Obsolète, voir* RFC6331)

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

[RFC5234] D. Crocker, P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

8.2 Références pour information

[RFC5801] S. Josefsson, N. Williams, "Utilisation des mécanismes génériques d'interface d'application de service de sécurité (GSS-API) dans la couche simple d'authentification et de sécurité (SASL) : Famille de mécanismes GS2", juillet 2010. *(P. S. ; MàJ par* RFC9266*)*

[RFC2203] M. Eisler, A. Chiu, L. Ling, "Spécification du protocole RPCSEC_GSS", septembre 1997. *(P.S.)*

[RFC2606] D. Eastlake 3rd et A. Panitz, "Noms réservés de niveau supérieur du DNS", BCP 32, juin 1999.

[RFC3530] S. Shepler et autres, "Protocole de système de fichiers réseau (NFS) v. 4", avril 2003. (*P.S. ; remplacée par* RFC7530)

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4422] A. Melnikov et K. Zeilenga, éd, "Authentification simple et couche de sécurité (SASL)", juin 2006. *(P.S.)*

[RFC4752] A. Melnikov, éd., "Méthode d'utilisation de l'interface de programme d'application de service générique de sécurité (GSS-API) Kerberos v5 dans le mécanisme d'authentification simple et couche de sécurité (SASL)", novembre 2006.

Adresse des auteurs

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

Alexey Melnikov
Isode Ltd.
5 Castle Business Village,
36 Station Road
Hampton, Middlesex TW12 2BX
United Kingdom
mél : Alexey.Melnikov@isode.com

Déclaration complète de droits de reproduction