Groupe de travail Réseau
Request for Comments : 4785
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

U. Blumenthal, Intel Corporation
P. Goel, Intel Corporation
janvier 2007

Suites de chiffrement de clés pré partagées (PSK) avec chiffrement NULL pour la sécurité de la couche transport (TLS)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document spécifie des suites de chiffrement pour authentification seule (sans chiffrement) pour la clé pré partagée (PSK, *Pre-Shared Key*) fondée sur le protocole de sécurité de la couche transport (TLS, *Transport Layer Security*). Ces suites de chiffrement sont utiles quand l'authentification et la protection de l'intégrité sont désirées, mais que la confidentialité n'est pas nécessaire ou pas permise.

Table des matières

1. Introduction

La RFC sur la sécurité de la couche transport (TLS, *Transport Layer Security*) fondée sur la clé pré partagée (PSK, *Pre-Shared Key*) [RFC4279] spécifie des suites de chiffrement pour la prise en charge de TLS en utilisant des clés pré-partagées symétriques. Cependant, toutes les suites de chiffrement définies dans la [RFC4279] exigent le chiffrement. Il y a pourtant des cas où seules l'authentification et la protection de l'intégrité sont requises, et la confidentialité n'est pas nécessaire. Il y a aussi des cas où la confidentialité n'est pas permise - par exemple, pour des mises en œuvre qui doivent satisfaire à des restrictions d'importation dans certains pays. Même si aucun chiffrement n'est utilisé, ces suites de chiffrement prennent en charge l'authentification mutuelle du client et du serveur, et l'intégrité du message. Le présent document augmente la [RFC4279] en ajoutant trois suites de chiffrement supplémentaires (PSK, DHE_PSK, RSA_PSK) avec seulement l'authentification et l'intégrité – sans chiffrement. Le lecteur est supposé s'être familiarisé avec la [RFC4279] avant d'étudier le présent document.

1.1 Déclaration d'applicabilité

Les suites de chiffrement définies dans le présent document sont destinées à un ensemble assez limité d'applications,

impliquant généralement seulement un très petit nombre de clients et serveurs. Même dans ces environnements, d'autres solutions de remplacement peuvent être plus appropriées.

Si le but principal est d'éviter les infrastructures de clés publiques (PKI, *Public-key Infrastructure*) une autre possibilité qu'il vaut la peine de considérer est d'utiliser des certificats auto signés avec des empreintes de clé publique. Au lieu de configurer manuellement un secret partagé dans, par exemple, un fichier de configuration, une empreinte (hachage) de la clé publique de l'autre partie (ou d'un certificat) pourrait y être mis à la place.

Il est aussi possible d'utiliser les suites de chiffrement de mot de passe sécurisé à distance (SRP, *Secure Remote Password*) pour l'authentification du secret partagé [RFC5054]. SRP a été conçu pour être utilisé avec des mots de passe, et il incorpore la protection contre les attaques de dictionnaire. Cependant, il est plus coûteux en calcul que les suites de chiffrement PSK de la [RFC4279].

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. Usage du chiffrement

Les trois nouvelles suites de chiffrement proposées ici correspondent aux trois suites de chiffrement définies dans la [RFC4279], sauf que les suites sont définies avec le chiffrement nul.

Les suites de chiffrement définies ici utilisent les options suivantes pour l'échange de clé et la partie hachage du protocole :

Suite de chiffrement	**Échangede clé**	**Chiffrement**	**Hachage**
TLS_PSK_WITH_NULL_SHA	PSK	NUL	SHA
TLS_DHE_PSK_WITH_NULL_SHA	DHE_PSK	NUL	SHA
TLS_RSA_PSK_WITH_NULL_SHA	RSA_PSK	NUL	SHA

Pour la signification du terme PSK, se référer à la Section 1 de la [RFC4279]. Pour la signification des termes DHE, RSA, et SHA, se référer aux Appendices A.5 et B de la [RFC4346].

4. Considérations sur la sécurité

Comme avec tous les schémas qui impliquent des clés partégées, une attention particulière devrait être apportée à protéger les valeurs partagées et à limiter leur exposition dans le temps. Comme le présent document complète la [RFC4279], tout ce qui est déclaré dans sa section de considérations sur la sécurité s'applique ici. De plus, comme les suites de chiffrement définies ici ne prennent pas en charge la confidentialité, on devrait veiller à ne pas envoyer d'informations de données sensibles (comme des mots de passe) sur des connexions protégées par une des suites de chiffrement définies dans le présent document.

5. Considérations relatives à l'IANA

Le présent document définit trois nouvelles suites de chiffrement dont les valeurs sont dans le registre des suites de chiffrement TLS défini dans la [RFC4346].

CipherSuite TLS_PSK_WITH_NULL_SHA = { 0x00, 0x2C } ;
CipherSuite TLS_DHE_PSK_WITH_NULL_SHA = { 0x00, 0x2D } ;
CipherSuite TLS_RSA_PSK_WITH_NULL_SHA = { 0x00, 0x2E } ;

6. Remerciements

Les suites de chiffrement définies dans le présent document sont fondées sur la [RFC4279] et s'ajoutent à elle.

7. Références

7.1 Références normatives

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

[RFC4279] P. Eronen et H. Tschofenig, éd., "Suites de chiffrement de clés pré-partagées pour la sécurité de la couche Transport (TLS)", décembre 2005. *(P.S.)*

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

7.2 Références pour information

[RFC5054] D. Taylor et autres, "Utilisation du protocole de mot de passe sécurisé à distance (SRP) pour l'authentification TLS", novembre 2007. *(Information)*

Adresse des auteurs

Uri Blumenthal
Intel Corporation
1515 State Route 10,
PY2-1 10-4
Parsippany, NJ 07054
USA
mél : urimobile@optonline.net

Purushottam Goel
Intel Corporation
2111 N.E. 25 Ave.
Hillsboro, OR 97124
USA
mél : Purushottam.Goel@intel.com

Déclaration complète de droits de reproduction

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 le 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 actuellement fourni par la Internet Society.