Groupe de travail Réseau
Request for Comments : 3749
Catégorie : En cours de normalisation

S. Hollenbeck, VeriSign, Inc.
mai 2004
Traduction Claude Brière de L'Isle

Méthodes de compression du protocole de sécurité de la couche Transport

Résumé
Le protocole de sécurité de la couche Transport (TLS, *Transport Layer Security*) (RFC 2246) comporte un dispositif pour négocier le choix d'une méthode de compression des données sans perte au titre du protocole de prise de contact TLS et pour ensuite appliquer l'algorithme associé à la méthode choisie au titre du protocole enregistrement TLS. TLS définit une méthode standard de compression qui spécifie que les données échangées via le protocole d'enregistrement ne seront pas compressées. Le présent document décrit une méthode de compression supplémentaire associée à un algorithme de compression de données sans perte à utiliser avec TLS, et il décrit une méthode pour la spécification de méthodes de compression TLS supplémentaires.

Table des matières

1. Introduction

Le protocole de sécurité de la couche Transport (TLS) (RFC 2246, [2]) comporte des dispositifs de négociation d'une méthode de compression des données sans perte au titre du protocole TLS de prise de contact et ensuite d'appliquer l'algorithme associé à la méthode choisie au titre du protocole d'enregistrement TLS. TLS définit une méthode de compression standard, CompressionMethod.null, qui spécifie que les données échangées via le protocole d'enregistrement ne seront pas compressées. Bien que cette seule méthode de compression aide à garantir que les mises en œuvre TLS sont interopérables, l'absence de méthodes de compression standard supplémentaires a limité la capacité à développer des mises en œuvre interopérables qui incluent la compression des données.

TLS est utilisé très largement pour sécuriser les connexions client-serveur sur la Toile mondiale. Bien que ces connexions puissent souvent être caractérisées comme brèves et échangeant des quantités de données relativement petites, TLS est aussi utilisé dans des environnements où les connexions peuvent être de longue durée et où la quantité de données échangées peut atteindre de milliers ou des millions d'octets. XML [4], par exemple, connaît une utilisation croissante

comme méthode de représentation des données sur l'Internet, et XML tend à être prolixe. La compression au sein de TLS est un moyen d'aider à réduire la bande passante et les exigences de latence associés à l'échange de grandes quantités de données tout en préservant les services de sécurité fournis par TLS.

Le présent document décrit une méthode supplémentaire de compression associée à un algorithme de compression de données sans perte à utiliser avec TLS. La normalisation des formats de données compressées et des algorithmes de compression associés à cette méthode de compression est en dehors du domaine d'application du présent document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la RFC 2119 [1].

2. Méthodes de compression

TLS [2] inclut la structure de méthode de compression suivante dans les paragraphes 6.1 et 7.4.1.2 et l'Appendice A.4.1 et A.6 :
enum { null(0), (255) } CompressionMethod;
qui permettre la spécification ultérieure d'un maximum de 256 méthodes de compression différentes. Cette définition est mise à jour pour distinguer trois zones de gamme de valeurs admissibles :

1. Les valeurs décimales de 0 (zéro) à 63 (0x3F) inclus sont réservées pour les protocoles de l'IETF en cours de normalisation.

2. Les valeurs de 64 décimal (0x40) à 223 décimal (0xDF) inclus sont réservées pour l'allocation à des méthodes qui ne sont pas en cours de normalisation.

3. Les valeurs de 224 décimal (0xE0) à 255 décimal (0xFF) inclus sont réservées pour utilisation privée.

Des informations supplémentaires pour décrire le rôle de l'IANA dans l'allocation des identifiants de méthode de compression sont données à la Section 5.

De plus, cette définition est mise à jour pour inclure l'allocation d'un identifiant pour la méthode de compression DEFLATE :

enum { null(0), DEFLATE(1), (255) } CompressionMethod;

Comme décrit à la section 6 de la RFC 2246 [2], TLS est un protocole à états pleins. Les méthodes de compression utilisées avec TLS peuvent être à états pleins (le compresseur conserve son état à travers tous les enregistrements compressés) ou sans état (le compresseur compresse chaque enregistrement de façon indépendante), mais il semble y avoir peu d'avantages connus à utiliser une méthode de compression sans états dans TLS.

La méthode de compression DEFLATE décrite dans le présent document est à états pleins. Il est RECOMMANDÉ que les autres méthodes de compression qui pourraient être normalisées à l'avenir soient elles aussi à états pleins.

Les algorithmes de compression peuvent à l'occasion amplifier plutôt que compresser les données d'entrée. Une méthode de compression qui excède les limites d'expansion décrites au paragraphe 6.2.2 de la RFC 2246 [2] NE DOIT PAS être utilisée avec TLS.

2.1 Compression DEFLATE

La méthode de compression et le format de codage DEFLATE sont décrits dans la RFC 1951 [5]. On trouve des exemples d'utilisation de DEFLATE dans les protocoles de l'IETF de la RFC 1979 [6], la RFC 2394 [7], et la RFC 3274 [8].

DEFLATE permet au compresseur d'envoi de choisir parmi plusieurs options de fournir divers taux de compression, de vitesse de traitement, et d'exigences de mémoire. Le décompresseur receveur DOIT s'ajuster automatiquement aux paramètres choisis par l'envoyeur. Toutes les données qui ont été soumises à la compression DOIVENT être incluses dans le résultat compressé, sans qu'aucune données ne soient retenues pour être incluses dans une charge utile de sortie ultérieure. La purge permet de s'assurer que chaque charge utile de paquet compressé peut être complètement décompressée.

3. Histoire de la compression et du traitement de paquet

Certaines méthodes de compression ont la capacité à maintenir les informations d'état/historique lors de la compression et décompression des charges utiles de paquet. L'historique de compression permet de réaliser un plus fort taux de compression sur un flux par rapport à une compression paquet par paquet, mais entretenir un historique à travers les paquets implique qu'un paquet puisse contenir les données nécessaires pour décompresser complètement les données contenues dans un paquet différent. La maintenance de l'historique exige donc à la fois une liaison fiable et une livraison des paquets en séquence. Comme TLS et les protocoles de couche inférieure fournissent une livraison fiable et en séquence des paquets, les informations d'historique de compression PEUVENT être conservées et exploitées si c'est accepté par la méthode de compression.

Comme décrit à la section 7 de la RFC 2246 [2], TLS permet que plusieurs connexions soient instanciées en utilisant la même session grâce au dispositif de reprise du protocole de prise de contact TLS. La reprise de session a des implications opérationnelles lorsque plusieurs méthodes de compression sont disponibles au sein de la session. Par exemple, les équilibreurs de charge vont devoir entretenir des informations d'état supplémentaires si l'état de compression n'est pas libéré lors de la reprise d'une session. Il en résulte que les restrictions suivantes DOIVENT être observées à la reprise d'une session :

1. L'algorithme de compression DOIT être conservé lors de la reprise d'une session.

2. L'état/historique de compression DOIT être libéré lors d'une reprise de session.

4. Considérations pour l'internationalisation

Les identifiants de méthode de compression spécifiés dans le présent document sont des numéros lisibles par une machine. Par conséquent, les questions d'internationalisation et de localisation humaine ne sont pas abordées.

5. Considérations relatives à l'IANA

La Section 2 du présent document décrit un registre d'identifiants de méthode de compression qui sera tenu par l'IANA, y compris l'allocation d'un identifiant pour la méthode de compression DEFLATE. Les valeurs d'identifiant de la gamme 0 à 63 (décimal) inclus sont allouées via l'action de normalisation de la RFC 2434 [3]. Les valeurs dans la gamme 64 à 223 (décimal) inclus sont allouées via l'exigence d'une spécification de la RFC 2434 [3]. Les valeurs d'identifiant de 224 à 255 (décimal) inclus sont réservées pour l'utilisation privée de la RFC 2434 [3].

6. Considérations pour la sécurité

Le présent document n'introduit aucun sujet qui altère le modèle de menaces traité par TLS. Les considérations pour la sécurité décrites dans la RFC 2246 [2] s'appliquent aussi ici.

Cependant, combiner la compression et le chiffrement peut parfois révéler des informations qui ne l'auraient pas été sans la compression : les données qui ont la même longueur avant la compression peuvent avoir une longueur différente après la compression, aussi des adversaires qui observent la longueur des données compressées peuvent être capables de déduire des informations sur les donnés non compressées correspondantes. Certaines suites de chiffrement de cryptage symétrique ne cachent pas du tout la longueur des données qui ont subi un chiffrement symétrique. D'autres la cachent dans une certaine mesure, mais pas complètement. Par exemple, des suites de chiffrement qui utilisent le chiffrement de flux sans bourrage ne cachent pas du tout la longueur ; les suites de chiffrement qui utilisent le chaînage de bloc de chiffrement CBC, *Cipher Block Chaining*) avec bourrage fournissent une certaine dissimulation de longueur, qui dépend de la façon dont est choisie la quantité de bourrage. L'utilisation de la compression TLS DEVRAIT prendre en compte que la longueur des données compressées peut révéler plus d'informations que la longueur des données originales non compressées.

Les algorithmes de compression tendent à être mathématiquement complexes et enclins aux erreurs de mise en œuvre. Une erreur de mise en œuvre qui peut produire un dépassement de mémoire tampon introduit un risque potentiel pour la sécurité pour les langages de programmation et les systèmes d'exploitation qui ne fournissent pas de protections contre les dépassements de mémoire. Une considération attentive devrait donc être apportée aux protections contre les erreurs de mise en œuvre qui introduisent des risques pour la sécurité.

Comme décrit à la Section 2, les algorithmes de compression peuvent à l'occasion amplifier, plutôt que compresser, les

données d'entrée. Cette caractéristique introduit une capacité à construire des données pirates qui ont une expansion énorme lorsqu'elles sont compressées ou décompressées. La RFC 2246 décrit plusieurs méthodes pour améliorer cette sorte d'attaque. D'abord, la compression doit être sans perte. Ensuite, une limite (1 024 octets) est fixée à la quantité d'accroissement admis de la longueur du contenu de la compression. Finalement, une limite (2^14 octets) est fixée à la longueur totale du contenu. Voir au paragraphe 6.2.2 de la RFC 2246 [2] les détails complets.

7. Remerciements

Les concepts décrits dans le présent document ont été discutés à l'origine sur la liste de diffusion du groupe de travail TLS de l'IETF en décembre, 2000. L'auteur remercie de leurs contributions à cette discussion Jeffrey Altman, Eric Rescorla, et Marc Van Heyningen. Des suggestions ultérieures fournies par Tim Dierks, Pasi Eronen, Peter Gutmann, Elgin Lee, Nikos Mavroyanopoulos, Alexey Melnikov, Bodo Moeller, Win Treese, et l'IESG ont été incorporées dans le présent document.

8. Références

8.1 Références normatives

[1] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[2] T. Dierks et C. Allen, "Protocole TLS version 1.0", RFC 2246, janvier 1999. *(Rendue obsolète par la RFC 4346, elle-même rendue obsolète par la RFC 5246 août 2008)*

[3] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction de la section Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 2434, octobre 1998.

8.2 Références informatives

[4] T. Bray, J. Paoli, C. Sperberg-McQueen et E. Maler, "Langage de balisage extensible (XML) 1.0 (2e éd.)", W3C REC-xml, octobre 2000, <http://www.w3.org/TR/REC-xml>.

[5] P. Deutsch, "Spécification du format de données compressées DEFLATE version 1.3", RFC 1951, mai 1996.

[6] J. Woods, "Protocole Deflate PPP", RFC 1979, août 1996.

[7] R. Pereira, "Compression de charge utile IP utilisant DEFLATE", RFC 2394, décembre 1998.

[8] P. Gutmann, "Type de contenu de données compressées pour la syntaxe de message cryptographique (CMS)", RFC 3274, juin 2002.

Adresse de l'auteur

Scott Hollenbeck
VeriSign, Inc.
21345 Ridgetop Circle
Dulles, VA 20166-6503
US
mél : shollenbeck@verisign.com

Déclaration complète de droits de reproduction

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 pourrait 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 actuellement fourni par l'Internet Society.