Groupe de travail Réseau
Request for Comments : 3436
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

A. Jungmaier, University of Essen
E. Rescorla, RTFM Inc.
M. Tuexen, Siemens AG
décembre 2002

Sécurité de la couche transport sur le protocole de transmission de contrôle de flux

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître 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 décrit l'usage du protocole de sécurité de la couche transport (TLS, *Transport Layer Security*) tel que défini dans la [RFC2246], sur le protocole de transmission de contrôle de flux (SCTP, *Stream Control Transmission Protocol*) tel que défini dans les [RFC2960] et [RFC3309].

L'utilisateur de TLS peut tirer parti des caractéristiques fournies par SCTP, à savoir la prise en charge de plusieurs flux pour éviter le blocage de tête de ligne et la prise en charge du multi-rattachement pour assurer la tolérance de faute au niveau réseau.

De plus, la discussion des extensions à SCTP est aussi assurée, visant particulièrement la prise en charge de la reconfiguration dynamique des adresses IP.

1. Introduction

1.1 Généralités

Le présent document décrit l'utilisation du protocole de sécurité de la couche transport (TLS, *Transport Layer Security*) tel que défini dans la [RFC2246], sur le protocole de transmission de contrôle de flux (SCTP, *Stream Control Transmission Protocol*), défini dans les [RFC2960] et [RFC3309].

TLS est conçu pour fonctionner par dessus un protocole de transport en mode de flux d'octets fournissant une livraison fiable, en séquence. Donc, TLS est actuellement principalement utilisé par dessus le protocole de contrôle de transmission (TCP, *Transmission Control Protocol*), tel que défini dans la [RFC0793].

Si on compare TCP et SCTP, ce dernier fournit des caractéristiques supplémentaires et le présent document montre comment TLS devrait être utilisé avec SCTP pour fournir certaines de ces caractéristiques supplémentaires à l'utilisateur de TLS.

Le présent document définit :
- comment utiliser la caractéristique multi flux de SCTP,
- comment traiter la nature en mode message de SCTP.

On devrait noter que l'utilisateur de TLS peut tirer parti de la prise en charge du multi rattachement de SCTP. La reconfiguration dynamique des adresses IP, telle qu'elle est actuellement discutée, peut aussi être utilisée avec la solution décrite.

La méthode décrite dans ce document n'exige aucun changement de TLS ni de SCTP. Il est seulement demandé que les mises en œuvre de SCTP prennent en charge la caractéristique facultative de fragmentation des messages de l'usager SCTP.

1.2 Terminologie

Le présent document utilise les termes suivants :

Association : une association SCTP.

Connexion : une connexion TLS.

Session : une session TLS.

Flux : un flux unidirectionnel d'une association SCTP. Il est identifié de façon univoque par un identifiant de flux.

1.3 Abréviations

MTU *(Maximum Transmission Unit)* : unité maximale de transmission

SCTP *(Stream Control Transmission Protocol)* : protocole de transmission de contrôle de flux

TCP *(Transmission Control Protocol)* : protocole de contrôle de transmission

TLS *(Transport Layer Security)* : sécurité de la couche transport

2. Conventions

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. Exigences de SCTP

3.1 Nombre de flux entrants et sortants

Une association entre les points d'extrémité A et Z donne un flux de A à Z et m flux de Z vers A.

Une paire consistant en deux flux avec le même identifiant de flux est considérée et utilisée comme un flux bidirectionnel.

Donc, une association SCTP peut être considérée comme un ensemble de min(n,m) flux bidirectionnels et (max(n,m) - min(n,m)) flux unidirectionnels.

3.2 Fragmentation des messages d'utilisateur

Pour éviter d'avoir à connaître et traiter la MTU au sein de TLS, SCTP DOIT fournir la fragmentation des messages d'utilisateur, qui est une caractéristique facultative de la [RFC2960]. Comme SCTP est un protocole en mode message, il doit être capable de transmettre tous les enregistrements TLS comme des messages d'utilisateur SCTP. Donc, la longueur maximale prise en charge des messages d'utilisateur SCTP DOIT être d'au moins 2^14 + 2048 + 5 = 18437 octets, qui est la longueur maximale d'un TLSCiphertext, comme défini dans la [RFC2246].

Prière de noter qu'une mise en œuvre SCTP peut avoir besoin de prendre en charge l'API de livraison partielle pour être capable d'accepter le transport de messages d'utilisateur de cette taille.

Donc, SCTP prend soin de fragmenter et réassembler les enregistrements TLS afin d'éviter la fragmentation IP.

4. Exigences de TLS

4.1 Suites de chiffrement prises en charge

Une mise en œuvre de TLS pour TLS sur SCTP DOIT prendre en charge au moins la suite de chiffrement TLS_RSA_WITH_AES_128_CBC_SHA comme défini dans la [RFC3268].

5. Connexions et flux bidirectionnels

TLS fait usage d'un flux bidirectionnel en établissant une connexion sur lui. Cela signifie que le nombre de connexions pour une association est limité par le nombre de flux bidirectionnels.

Le protocole de prise de contact TLS est utilisé séparément sur chaque flux bidirectionnel. Chaque prise de contact peut être :
- une prise de contact complète,
- ou une prise de contact abrégée qui reprend une session TLS avec un identifiant de session provenant d'une autre connexion (sur la même association, ou sur une autre).

Après l'achèvement de la prise de contact pour une connexion, le flux bidirectionnel peut être utilisé pour la transmission des données d'utilisateur fondée sur TLS. On devrait aussi noter que les prises de contact pour les différentes connexions sont indépendantes et peuvent être différées jusqu'à ce que le flux bidirectionnel soit utilisé pour la transmission des données d'utilisateur.

6. Usage des flux bidirectionnels

Il n'est pas exigé que tous les flux bidirectionnels soient utilisés pour la transmission des données d'utilisateur fondée sur TLS. Si TLS n'est pas utilisé, elle est appelée transmission de données d'utilisateur fondée sur SCTP.

6.1 Transmission de données d'utilisateur fondée sur SCTP

Si un flux bidirectionnel n'est pas utilisé pour une communication fondée sur TLS, il n'y a pas de restriction aux caractéristiques fournies par SCTP pour la transmission de données d'utilisateur fondée sur SCTP.

6.2 Transmission de données d'utilisateur fondée sur TLS

En général, le flux bidirectionnel sera utilisé pour la transmission de données d'utilisateur fondée sur TLS et elle NE DEVRAIT PAS être utilisée pour la transmission de données d'utilisateur fondée sur SCTP. L'exception à cette règle est pour les protocoles qui contiennent des mécanismes de mise à niveau de TLS, comme ceux de mise à niveau de HTTP [RFC2817] et de SMTP sur TLS [RFC3207].

TLS exige que le transport sous-jacent délivre les enregistrements TLS en séquence stricte. Donc, la caractéristique "livraison en désordre" de SCTP NE DOIT PAS être utilisée sur les flux qui sont utilisés pour la transmission de données d'utilisateur fondée sur TLS. Pur la même raison, les enregistrements TLS livrés à SCTP pour transmission NE DOIVENT PAS avoir une durée de vie limitée.

7. Usage des flux unidirectionnels

Les flux unidirectionnels ne peuvent pas être utilisés pour la transmission de données d'utilisateur fondée sur TLS. Néanmoins, ils peuvent être utilisés sans aucune restriction pour les communications fondées sur SCTP.

8. Exemples

Dans ces exemples, on considère le cas d'une association avec deux flux bidirectionnels.

8.1 Deux flux bidirectionnels avec prise de contact entière

Juste après l'établissement de l'association, le client envoie deux messages ClientHello sur les flux bidirectionnels 0 et 1. Après avoir réalisé une pleine prise de contact sur chaque flux bi directionnel, la transmission de données d'utilisateur fondée sur TLS peut avoir lieu sur ce flux. Il est possible que sur le flux bidirectionnel 0, la prise de contact ait été achevée et que la transmission de données d'utilisateur soit en cours, tandis que sur le flux bidirectionnel 1, la prise de contact n'a pas été

achevée, ou vice versa.

8.2 Deux flux bidirectionnels avec une prise de contact abrégée

Après l'établissement de l'association, le client commence une pleine prise de contact sur le flux bidirectionnel 0. Le serveur fournit un identifiant de session qui permet la reprise de session. Après l'achèvement de la pleine prise de contact, le client initie une prise de contact abrégée sur le flux bidirectionnel 1, en utilisant l'identifiant de session provenant de la prise de contact effectuée sur le flux bidirectionnel 0. Les données d'utilisateur peuvent être transmises sur le flux bidirectionnel 0, mais pas sur le flux bidirectionnel 1 dans cet état. Après achèvement de la prise de contact abrégée sur le flux bidirectionnel 1, les données d'utilisateur peuvent être transmises sur les deux flux.

La décision d'utiliser ou non la prise de contact abrégée durant la phase d'établissement d'une connexion TLS sur une association SCTP dépend de plusieurs facteurs :
- la complexité et la durée du traitement de la prise de contact initiale 'aussi déterminée par le nombre de connexions),
- les performances du réseau (temps d'aller-retour, bande passante).

Les prises de contact abrégées peuvent réduire considérablement la complexité de calcul de la prise de contact, dans le cas où c'est une ressource limitée. Si un grand nombre de connexions doivent être établies, il peut être avantageux d'utiliser la caractéristique de reprise de session TLS. D'un autre côté, avant que puisse avoir lieu une prise de contact abrégée, une pleine prise de contact doit avoir été achevée. Dans les réseaux qui ont de longs délais d'aller-retour, il peut être plus favorable d'effectuer en parallèle un certain nombre de pleines prises de contact. Donc, les deux possibilités sont permises.

8.3 Deux flux bidirectionnels avec prise de contact abrégée différée

Cet exemple ressemble au précédent, mais après l'achèvement de la pleine prise de contact sur le flux bidirectionnel 0, la prise de contact abrégée sur le flux bidirectionnel 1 n'est pas commencée immédiatement. Le flux bidirectionnel 0 peut être utilisé pour la transmission de données d'utilisateur. C'est seulement lorsque l'usager veut transmettre des données sur le flux bidirectionnel 1 que la prise de contact abrégée est initiée pour le flux bidirectionnel 1.

Cela permet à l'usager de TLS de demander un grand nombre de flux bidirectionnels sans avoir à fournir toutes les ressources au démarrage de l'association si tous les flux bidirectionnels sont utilisés depuis le tout début.

8.4 Deux flux bidirectionnels sans pleine prise de contact

Cet exemple est comme les second et troisième, mais une prise de contact abrégée est utilisée pour les deux flux bidirectionnels. Cela requiert l'existence d'un identifiant de session valide à partir des connexions traitées par une autre association.

9. Considérations sur la sécurité

Utiliser TLS par dessus SCTP ne génère aucun nouveau problème de sécurité au delà de ceux exposés dans la [RFC2246] et la [RFC2960].

Il est possible d'authentifier les points d'extrémité TLS sur la base des adresses IP dans les certificats. À la différence de TCP, les associations SCTP peuvent utiliser plusieurs adresses par point d'extrémité SCTP. Donc, il est possible que les enregistrements TLS soient envoyés d'une adresse IP différente de celle originellement authentifiée. Ceci n'est pas un problème pourvu qu'aucune décision de sécurité ne soit prise sur la base de cette adresse IP. Ceci est un cas particulier d'une règle générale : toutes les décisions devraient se fonder sur l'identité authentifiée de l'homologue, et non sur son identité de couche transport.

10. Remerciements

Les auteurs tiennent à remercier P. Calhoun, J. Wood, et de nombreux autres pour leurs précieux commentaires et suggestions.

11. Références

11.1 Références normatives

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3268] P. Chown, "Suites de chiffrement de la norme de chiffrement évolué (AES) pour la sécurité de la couche Transport (TLS)", juin 2002. (*Obsolète, voir* RFC5246) *(P.S.)*

[RFC3309] J. Stone, R. Stewart, D. Otis, "Changement de somme de contrôle du protocole de transmission de commandes de flux (SCTP)". septembre 2002. (*Obsolète, voir* RFC4960) *(P.S.)*

11.2 Références pour information

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. *(Remplace* RFC1602, RFC1871) (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378, RFC6410)

[RFC2817] R. Khare, S. Lawrence, "Mise à niveau de TLS au sein de HTTP/1.1", mai 2000. *(P.S.)*

[RFC3207] P. Hoffman, "Extension de service SMTP pour un SMTP sécurisé sur TLS", février 2002. *(P.S.)*

12. Adresses des auteurs

Andreas Jungmaier
University of Essen
Networking Technology Group at the IEM
Ellernstrasse 29
D-45326 Essen
Germany
téléphone : +49 201 1837667
mél : ajung@exp-math.uni-essen.de

Eric Rescorla
RTFM, Inc.
2064 Edgewood Drive
Palo Alto, CA 94303
USA
téléphone : +1 650-320-8549
mél : ekr@rtfm.com

Michael Tuexen
Siemens AG
D-81359 Munich
Germany
téléphone : +49 89 722 47210
mél : Michael.Tuexen@siemens.com

13. Déclaration complète de droits de reproduction

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.

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.