Groupe de travail Réseau
Request for Comments : 5238
Catégorie : Sur la voie de la normalisation

T. Phelan, Sonus Networks
mai 2008
Traduction Claude Brière de L'Isle

Sécurité de la couche de transport de datagrammes (DTLS) sur le protocole de contrôle d'encombrement de datagrammes (DCCP)

Résumé
Le présent document spécifie l'utilisation de la sécurité de la couche de transport de datagrammes (DTLS, *Datagram Transport Layer Security*) sur le protocole de contrôle d'encombrement de datagrammes (DCCP, *Datagram Congestion Control Protocol*). DTLS assure la confidentialité des communications pour les applications qui utilisent des protocoles de transport de datagrammes et permettent aux applications de client/serveur de communiquer d'une façon conçue pour empêcher l'espionnage et détecter l'altération ou la falsification de message. DCCP est un protocole de transport qui fournit un service de datagrammes fiable à encombrement contrôlé.

Table des matières

1. Introduction

Le présent document spécifie comment porter des charges utiles d'application avec la sécurité de la couche de transport de datagrammes (DTLS, *Datagram Transport Layer Security*) comme spécifié dans la [RFC4347], dans le protocole de contrôle d'encombrement de datagrammes (DCCP, *Datagram Congestion Control Protocol*) comme spécifié dans la [RFC4340].

DTLS est une adaptation de la sécurité de la couche de transport (TLS, *Transport Layer Security)* [RFC4346] qui modifie TLS pour l'utilisation avec le protocole non fiable de transport UDP. TLS est un protocole qui permet aux applications de client/serveur de communiquer d'une façon conçue pour empêcher l'espionnage et détecter l'altération et la falsification de message. DTLS peut être vu comme TLS plus des adaptations pour la fiabilité.

DCCP fournit un service de transport non fiable, similaire à UDP, mais avec un contrôle d'encombrement adaptatif, similaire à celui de TCP et du protocole de transmission de contrôle de flux (SCTP, *Stream Control Transmission*

Protocol). DCCP peut être vu également comme UDP plus le contrôle d'encombrement ou comme TCP moins la fiabilité (bien que, à la différence de TCP, DCCP offre de nombreux algorithmes de contrôle d'encombrement).

La combinaison de DTLS et de DCCP va offrir des capacités de sécurité du transport aux applications qui utilisent DCCP, similaires à celles disponibles pour TCP, UDP, et SCTP.

2. Terminologie

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 le BCP 14, [RFC2119].

3. DTLS sur DCCP

L'approche est ici très directe – les enregistrements DTLS sont transmis dans les champs de données d'application des paquets DCCP-Data et DCCP-DataAck (dans la suite de ce document on suppose que "paquet de données DCCP" recouvre "paquet DCCP-Data ou DCCP-DataAck"). Plusieurs enregistrements DTLS PEUVENT être envoyés dans un paquet de données DCCP, pour autant que le paquet résultant soit dans l'unité de transfert maximum de chemin (PMTU, *Path Maximum Transfer Unit*) actuellement en vigueur pour les paquets de données normaux, si la fragmentation n'est pas permise (le bit Ne pas fragmenter (DF, *Don't Fragment*) est établi pour IPv4 ou pas d'en-têtes d'extension de fragmentation ne sont utilisés pour IPv6) ou dans la taille maximum de paquet DCCP actuelle si la fragmentation est permise (voir plus d'informations au paragraphe 3.5 sur la découverte de la PMTU). Un seul enregistrement DTLS DOIT être entièrement contenu dans un seul paquet de données DCCP ; il NE DOIT PAS être partagé sur plusieurs paquets.

3.1 DCCP et numéros de séquence DTLS

DCCP et DTLS utilisent tous deux des numéros de séquence dans leurs enregistrements de paquets. Ces numéros de séquence servent un peu, mais pas complètement, à des fonctions de recouvrement. Par conséquent, il n'y a pas de connexion entre le numéro de séquence d'un paquet DCCP et le numéro de séquence d'un enregistrement DTLS contenu dans ce paquet, et il n'y a pas de connexion entre les caractéristiques relatives aux numéros de séquence comme la synchronisation DCCP et la protection contre la répétition de DTLS.

3.2 DCCP et prises de contact de connexion DTLS

À la différence de UDP, DCCP est en mode connexion, et a une procédure de prise de contact de connexion qui précède la transmission des paquets de données DCCP et d'accusé de réception de données DCCP. DTLS est aussi en mode connexion, et a une procédure de prise de contact à lui qui doit précéder la transmission des informations d'application réelles. En utilisant la règle de transposition des enregistrements DTLS en paquets de données DCCP et d'accusé de réception de données DCCP de la Section 3, les deux prises de contact doivent forcément se produire à la suite, avec la prise de contact DCCP en premier, suivie par la prise de contact DTLS. C'est comme fonctionne TLS sur TCP.

Cependant, les paquets de prise de contact DCCP Demande DCCP et Réponse DCCP ont des champs Données d'application et peuvent porter des données d'utilisateur durant la prise de contact DCCP, et cela crée une opportunité pour effectuer les prises de contact partiellement en parallèle. Les mises en œuvre de client DTLS PEUVENT choisir de transmettre un ou plusieurs enregistrements DTLS (contenant normalement des messages de prise de contact DTLS ou des parties de ceux-ci) dans le paquet Demande DCCP. Une mise en œuvre de serveur DTLS PEUT choisir de traiter ces enregistrements comme d'habitude, et si elle a un ou plusieurs enregistrements DTLS à envoyer en réponse (contenant normalement des messages de prise de contact DTLS ou des parties de ceux-ci) elles PEUVENT inclure ces enregistrements dans le paquet de réponse DCCP. Les serveurs DTLS PEUVENT aussi choisir de retarder la réponse jusqu'à la fin de la prise de contact DCCP et d'envoyer ensuite la réponse DTLS dans un paquet de données DCCP.

Noter que même si la prise de contact DCCP est un processus fiable (les messages de prise de contact DCCP sont retransmis comme nécessaire si des messages sont perdus) le transfert des données d'application dans les paquets Demande DCCP et Réponse DCCP n'est pas nécessairement fiable. Par exemple, une mise en œuvre de serveur DCCP est libre d'éliminer des données d'application reçues dans des paquets de demande DCCP. Et si des paquets de demande ou réponse DCCP doivent être retransmis, la mise en œuvre de DCCP peut choisir de ne pas inclure les données d'application présentes

dans le message initial.

Comme la prise de contact DTLS est aussi un processus fiable, elle va interopérer à travers la non fiabilité de livraison des données de DCCP (après tout, une des fonctions de base de DTLS est de fonctionner sur des transports non fiables). Si les enregistrements DTLS qui contiennent les messages de prise de contact DTLS sont perdus, ils vont être retransmis par DTLS.

Ceci est sans considération de si les messages ont été envoyés dans des paquets de demande/réponse DCCP ou des paquets de données DCCP. Cependant, la seule façon pour DTLS de retransmettre des enregistrements DTLS qui ont été à l'origine transmis dans des paquets de demande/réponse DCCP (et que eux ou leurs réponses ont été perdus) est d'attendre la fin de la prise de contact DCCP et de renvoyer les enregistrements dans des paquets de données DCCP. Ceci est dû à la caractéristique de DCCP que la prochaine opportunité d'envoyer des données après l'envoi de données dans une demande DCCP est seulement après l'achèvement de la prise de contact de connexion.

DCCP et DTLS utilisent des stratégies similaires pour la retransmission des messages de prise de contact. Si il n'y a pas de réponse à la demande d'origine (demande DCCP ou tout message de prise de contact DTLS où une réponse est attendue) dans normalement une seconde, le message est retransmis. Le temporisateur est ensuite doublé et le processus répété jusqu'à ce qu'une réponse soit reçue, ou qu'un délai maximum soit dépassé.

Donc, si des enregistrements DTLS sont envoyés dans un paquet Demande DCCP, et si le message Demande DCCP ou Réponse DCCP est perdu, les prises de contact DCCP et DTLS pourraient arriver en fin de temporisation sur des échelles similaires. Les paquets Demande DCCP vont être retransmis en fin de temporisation, mais les enregistrements DTLS ne peuvent pas être retransmis tant que la prise de contact DCCP n'est pas achevée (il n'y a pas de possibilité d'ajouter de nouvelles données d'application à une retransmission de demande DCCP). Afin d'éviter plusieurs retransmissions DTLS en file d'attente avant que la première retransmission puisse être envoyée, DTLS sur DCCP DOIT attendre jusqu'à la fin de la prise de contact DCCP avant de relancer son temporisateur de retransmission de prise de contact DTLS.

3.3 Effets du contrôle d'encombrement DCCP

Étant donnée la taille potentiellement grande des messages de prise de contact DTLS, il est possible que le contrôle d'encombrement DCCP puisse réduire la transmission de la prise de contact DTLS au point que le transfert ne puisse s'achever avant la fin de la temporisation DTLS et l'effet des procédures de retransmission. Ajouter des messages retransmis à une situation d'encombrement rendraient les choses pires et retarderait l'établissement de la connexion.

Noter qu'une application DTLS sur UDP qui transmet des données de prise de contact dans cette même situation du réseau ne va pas nécessairement recevoir un meilleur débit, et pourrait en fait subir un débit effectif pire.

Sans la régulation du démarrage lent et du contrôle d'encombrement, une application UDP pourrait rendre l'encombrement pire et diminuer le débit effectif qu'elle reçoit.

Comme déclaré dans la [RFC4347], "le mauvais traitement du temporisateur [de retransmission] peut conduire à de sérieux problèmes d'encombrement". Cela reste vrai pour DTLS sur DCCP comme ce l'est pour DTLS sur UDP.

Les mises en œuvre de DTLS sur DCCP DEVRAIENT prendre des mesures pour éviter de retransmettre une demande qui a été mise en file d'attente mais pas encore réellement transmise par DCCP, quand la mise en œuvre sous-jacente de DCCP peut fournir ces informations. Par exemple, DTLS pourrait retarder le début du temporisateur de retransmission jusqu'à ce que DCCP indique que le message a été transféré de DCCP à la couche IP.

En plus des problèmes de retransmission, si les besoins de débit des données d'application réelles diffèrent des besoins de la prise de contact DTLS, il est possible que le transfert de prise de contact puisse laisser le contrôle d'encombrement DCCP dans un état qui ne convient pas immédiatement pour les données d'application qui vont suivre. Par exemple, l'identifiant de contrôle d'encombrement (CCID, *Congestion Control Identifier*) 2 [RFC4341] utilise un algorithme d'augmentation additive/diminution multiplicative (AIMD, *Additive Increase Multiplicative Decrease*) similaire au contrôle d'encombrement TCP. Si il est utilisé, il est alors possible que le transfert d'une grosse prise de contact puisse causer une diminution multiplicative qui ne se serait pas produite avec les données d'application. L'application pourrait alors être réduite lors de l'attente qu'une augmentation ramène le débit à des niveaux acceptables.

Les applications où ce pourrait être un problème devraient envisager d'utiliser le CCID 3 DCCP ([RFC4342]). Le CCID 3 met en œuvre le contrôle de débit convivial sur TCP (TFRC, *TCP-Friendly Rate Control*) [RFC3448]. Le TFRC fait varier le débit permis plus lentement que l'AIMD et pourrait éviter des discontinuités possibles avec CCID 2.

3.4 Relations entre les connexions de sessions DTLS et les connexions DCCP

DTLS utilise les concepts de sessions et connexions. Une connexion DTLS est utilisée par les points d'extrémité de couche supérieure pour échanger des données sur un protocole de transport. Les sessions DTLS contiennent des informations d'état en antémémoire qui sont utilisées pour réduire le nombre d'allers-retours et la quantité de calcul requis pour créer plusieurs connexions DTLS entre les mêmes points d'extrémité.

Dans DTLS sur DCCP, une connexion DTLS est portée par une connexion DCCP. Souvent l'établissement de la connexion DCCP est immédiatement suivie par l'établissement de la connexion DTLS (soit en créant une nouvelle session DTLS avec prise de contact complète, soit en reprenant une session DTLS existante) et la terminaison de la connexion DTLS est immédiatement suivie par la terminaison de la connexion DCCP, mais ce n'est pas la seule possibilité.

La vie d'une connexion DTLS sur DCCP est complètement contenue dans la vie de la connexion DCCP sous-jacente ; une connexion DTLS ne peut pas continuer si sa connexion DCCP sous-jacente se termine. Cependant, plusieurs connexions DTLS peuvent être reprises à partir de la même session DTLS, chacune fonctionnant sur sa propre connexion DCCP. Les caractéristiques de reprise de session de DTLS sont largement utilisées, et cette situation va probablement se produire dans de nombreux cas d'utilisation. Il est aussi possible de reprendre une session DTLS avec une nouvelle connexion DTLS fonctionnant sur un transport différent.

Noter qu'il est possible qu'une application commence une connexion DCCP en transférant des paquets non protégés, et en passant ensuite à DTLS. Ceci va probablement être utile pour les applications qui voudraient négocier l'utilisation de DTLS et a des implications sur le choix du code de service DCCP. Voir plus d'informations au paragraphe 3.6.

De nombreuses interfaces de programmation d'application (API, *Application Programming Interface*) DTLS n'empêchent pas une application d'envoyer un mélange de paquets chiffrés et en clair sur la même connexion de transport. Les applications NE DOIVENT PAS envoyer des données non protégées sur une connexion DCCP alors qu'elle porte aussi une connexion DTLS, car cela présente une vulnérabilité aux attaques d'insertion de paquets.

De nombreuses API DTLS permettent aussi à une application de commencer plusieurs connexions DTLS en série sur une connexion de transport, avec la terminaison d'une connexion DTLS suivie par le début d'une autre. Le traitement d'une prise de contact DTLS fait une consommation relativement importante de CPU. Une application qui utilise cette stratégie est ouverte à un attaquant qui ouvre et arrête immédiatement les sessions de façon répétée. Donc, les applications qui utilisent cette stratégie DEVRAIENT trouver un moyen limiter la charge potentielle sur le système. Par exemple, l'application pourrait appliquer un délai minimum de une seconde entre les initiations de session.

3.5 Découverte de la PMTU

Chaque enregistrement DTLS doit tenir dans un seul paquet de données DCCP. Les paquets DCCP sont normalement transmis avec le bit DF (ne pas fragmenter) établi pour IPv4 (ou sans en-tête d'extension de fragmentation pour IPv6). À cause de cela, DCCP effectue la découverte de l'unité de transmission maximum de chemin (PMTU, *Path Maximum Transmission Unit*).

DTLS utilise aussi normalement le bit DF et effectue d'elle-même la découverte de la PMTU, en utilisant un algorithme très similaire à celui utilisé par DCCP. Une mise en œuvre de DTLS sur DCCP PEUT utiliser la valeur gérée par DCCP pour la PMTU et ne pas effectuer d'elle-même la découverte de la PMTU. Cependant, les mises en œuvre qui choisissent d'utiliser la valeur de PMTU gérée par DCCP DEVRAIENT continuer de suivre les procédures du paragraphe 4.1.1.1 de la [RFC4347] en ce qui concerne la fragmentation des messages de prise de contact durant les retransmissions de prise de contact. Autrement, une mise en œuvre de DTLS sur DCCP PEUT choisir d'utiliser ses propres calculs de découverte de PMTU, comme spécifié dans la [RFC4347], mais NE DOIT PAS utiliser une valeur supérieure à celle déterminée par DCCP.

Les mises en œuvre de DTLS permettent normalement aux applications de remettre l'estimation de PMTU à son état initial. Quand cela arrive, les mises en œuvre de DTLS sur DCCP DEVRAIENT aussi réinitialiser l'estimation de la PMTU DCCP.

Les mises en œuvre de DTLS permettent aussi parfois aux applications de contrôler l'utilisation du bit DF (sur IPv4) ou l'utilisation des en-têtes d'extension de fragmentation (sur IPv6). Les mises en œuvre de DTLS sur DCCP DEVRAIENT contrôler l'utilisation du bit DF ou des en-têtes d'extension de fragmentation par DCCP en accord avec les indications de

l'application, quand la mise en œuvre de DCCP le prend en charge. Noter que les mises en œuvre de DCCP ne sont pas obligées de prendre en charge l'envoi de paquets fragmentables.

Noter que la taille maximum de paquet (MPS, *Maximum Packet Size*) DCCP dans la [RFC4340] est bordée par l'état de contrôle d'encombrement actuel (la taille maximum de paquet de contrôle d'encombrement (CCMPS, *Congestion Control Maximum Packet Size*) dans la [RFC4340]). Même quand le bit DF n'est pas établi et quand les paquets DCCP peuvent donc être fragmentés, la MPS peut être inférieure aux 65 535 octets normalement utilisé dans UDP. Il est aussi possible que la CCMPS DCCP, et donc la MPS, varie au fil du temps lorsque les conditions d'encombrement changent. Les mises en œuvre de DTLS sur DCCP NE DOIVENT PAS utiliser une taille d'enregistrement DTLS supérieure à la MPS DCCP actuellement en vigueur.

3.6 Codes de service DCCP

La prise de contact de connexion DCCP inclut un champ appelé Code de service qui est destiné à décrire "le service de niveau application auquel l'application du client veut se connecter". De plus, les "codes de service sont destinés à fournir des informations sur le protocole d'application qu'une connexion a l'intention d'utiliser, aidant ainsi les boîtiers de médiation et réduisant la dépendance aux accès mondiaux bien connus" [RFC4340].

On s'attend à ce que de nombreux boîtiers de médiation donnent des privilèges différents aux applications fonctionnant avec DTLS sur DCCP par rapport à juste DCCP. Donc, les applications qui utilisent parfois DTLS sur DCCP et juste DCCP les autres fois DEVRAIENT enregistrer et utiliser des codes de service différents pour chaque mode de fonctionnement. Les applications qui utilisent DCCP et DTLS sur DCCP PEUVENT choisir d'écouter les connexions entrantes sur le même accès DCCP et distinguer le mode de la demande par le code de service offert.

Certaines applications peuvent commencer en utilisant DCCP sans DTLS, et ensuite passer facultativement à l'utilisation de DTLS sur la même connexion. Comme il n'y a pas de moyen de changer le code de service pour une connexion après son établissement, ces applications vont utiliser un nouveau code de service.

3.7 Nouvelles versions de DTLS

Avec le mûrissement de DTLS, des révisions et des mises à jour de la [RFC4347] peuvent être attendues. DTLS inclut des mécanismes pour identifier la version utilisée, et vraisemblablement de futures versions vont inclure des modes de rétrocompatibilité ou au moins ne vont pas permettre de connexions entre des versions différentes. Comme DTLS sur DCCP encapsule simplement de façon transparente les enregistrements DTLS, ces changements ne devraient pas affecter le présent document et les méthodes de ce document devraient s'appliquer aux futures versions de DTLS.

Donc, en l'absence d'une révision de ce document, on supposera qu'il s'applique à toutes les futures versions de DTLS. Ce document sera seulement révisé si une révision de DTLS ou DCCP (incluant ses CCID en rapport) rend nécessaire une révision de l'encapsulation.

Il est RECOMMANDÉ qu'une application migrant sur une nouvelle version de DTLS garde le même code de service DCCP utilisé pour l'ancienne version et permette à DTLS de fournir la prise en charge de la négociation de version. Si une nouvelle version de DTLS fournissait des nouvelles capacités significatives à l'application qui pourraient changer le comportement des boîtiers de médiation par rapport à l'application, un développeur d'application POURRAIT enregistrer un nouveau code de service.

4. Considérations sur la sécurité

Les considérations sur la sécurité pour DTLS sont spécifiées dans la [RFC4347] et pour DCCP dans la [RFC4340]. La combinaison de DTLS et de DCCP n'introduit pas de nouvelles considérations sur la sécurité.

5. Remerciements

L'auteur tient à remercier Eric Rescorla de ses conseils initiaux sur l'adaptation de DTLS à DCCP, et Gorry Fairhurst, Pasi Eronen, Colin Perkins, Lars Eggert, Magnus Westerlund, et Tom Petch de leurs commentaires sur le document.

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. *(MàJ par* RFC8174)

[RFC4340] E. Kohler et autres, "Protocole de contrôle d'encombrement de datagrammes (DCCP)", mars 2006. *(P.S.) (MàJ par* 6773)

[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)

[RFC4347] E. Rescorla, N. Modadugu, "Sécurité de la couche de transport de datagrammes", avril 2006. *(P.S.)*

6.2 Références pour information

[RFC3448] M. Handley, S. Floyd, J. Padhye, J. Widmer, "Contrôle de débit convivial sur TCP (TFRC) : Spécification du protocole", janvier 2003. (*Obsolète, voir* RFC5348) *(P.S.)*

[RFC4341] S. Floyd, E. Kohler, "Profil d'identifiant 2 de protocole de contrôle d'encombrement de datagrammes (DCCP) : Contrôle d'encombrement de style TCP", mars 2006. *(P.S. ; MàJ par* RFC8311)

[RFC4342] S. Floyd et autres, "Profil d'identifiant 3 de protocole de contrôle d'encombrement de datagrammes (DCCP) : Contrôle en douceur de débit TCP (TFRC)", mars 2006. *(P.S. ; MàJ par* RFC5348, RFC8311)

Adresse de l'auteur

Tom Phelan
Sonus Networks
7 Technology Park Dr.
Westford, MA USA 01886
téléphone : 978-614-8456
mél : tphelan@sonusnet.com

Déclaration complète de droits de reproduction

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.