Groupe de travail Réseau N. Williams, Sun
Request for Comments : 5056
Catégorie : Sur la voie de la normalisation novembre 2007
Traduction Claude Brière de L'Isle

Sur l'utilisation de liens de canaux pour sécuriser les canaux

Résumé
Le concept de lien de canal permet aux applications d'établir que les deux points d'extrémité d'un canal sûr à une couche du réseau sont les mêmes qu'à une couche supérieure en liant l'authentification à la couche supérieure au canal à la couche inférieure. Cela permet aux applications de déléguer la protection de session aux couches inférieures, ce qui présente divers avantages de performances. Le présent document discute et formalise le concept de lien de canal pour sécuriser les canaux.

Table des Matières

1. Introduction

Dans un certain nombre de situations, il est utile pour une application d'être capable de traiter l'authentification au sein de la couche d'application, tout en étant simultanément capable d'utiliser la sécurité de session ou de transport à une couche inférieure du réseau. Par exemple, IPsec [RFC4301] [RFC4302] [RFC4303] est sujet à être accéléré dans le matériel pour traiter de très hautes vitesses de liaison, mais les protocoles d'échange de clés IPsec et l'architecture IPsec ne sont pas utilisables comme mécanisme de sécurité au sein des applications, en particulier des applications qui ont des utilisateurs comme clients. Une méthode pour combiner la sécurité aux deux couches est donc intéressante. Pour permettre de faire cela en toute sécurité, il est nécessaire de "lier" ensemble les mécanismes -- de façon à éviter la vulnérabilité aux attaques

par interposition et permettre d'intégrer les mécanismes de façon transparente. C'est l'objectif des "liens de canaux".

Le terme de "lien de canal", tel qu'utilisé dans le présent document, découle de l'interface de programme d'application de service de sécurité générique (GSS-API, *Generic Security Service Application Program Interface*) [RFC2743], qui offre une facilité de lien de canal destinée à lier l'authentification GSS-API à des canaux sûrs aux couches de réseau inférieures. L'objet et l'avantage de la facilité de lien de canal GSS-API n'ont pas été discutés en profondeur, et certains détails sont restés non spécifiés. On trouve maintenant que ce concept peut être très utile, et donc on commence par une généralisation et la formalisation du "lien de canal" indépendamment de GSS-API.

Bien qu'inspirée par, et dérivée de, GSS-API, la notion de lien de canal décrite ici n'est pas du tout limitée à l'utilisation par les applications GSS-API. On envisage l'utilisation du lien de canal par des applications qui utilisent d'autres cadres de sécurité, comme l'authentification simple et couche de sécurité (SASL, *Simple Authentication et Security Layer*) [RFC4422] et méme des protocoles qui fournissent leurs propres mécanismes d'authentification (par exemple, les échanges de centre de distribution de clés (KDC, *Key Distribution Center*) dans Kerberos V [RFC4120]). On envisage aussi l'utilisation de la notion de lien de canal dans l'analyse des protocoles de sécurité.

Le but principal du lien de canal est d'être capable de déléguer la protection de la session cryptographique aux couches de réseau en dessous de l'application dans l'espoir d'être capable de mieux soutenir les mises en œuvre de matériel des protocoles cryptographiques. La Section 5 décrit des utilisations prévues du lien de canal. Aussi, certaines applications peuvent bénéficier de la réduction de la quantité d'état cryptographique actif, réduisant donc les frais généraux d'accès à cet état et, donc, l'impact de la sécurité sur la latence.

Le problème de sécurité critique à résoudre afin de réaliser une telle délégation de protection de session est de s'assurer qu'il n'y a pas d'interposé (MITM, *Man-In-The-Middle*) du point de vue de l'application, à la couche de réseau inférieure à laquelle la protection de session doit être déléguée.

Il peut fort bien y avoir un interposé, en particulier si la couche de réseau inférieure ne fournit pas d'authentification ou si il n'y a pas une connexion forte entre l'authentification ou les principaux utilisés à l'application et celle utilisée à la couche de réseau inférieure.

Même si de telles attaques de MITM semblent particulièrement difficlles à effectuer, les attaques doivent être empêchées pour certaines applications pour être capable de faire une utilisation efficace de technologies telles que IPsec [RFC2401] [RFC4301] ou HTTP avec TLS [RFC4346] dans certains contextes (par exemple, quand il n'y a pas d'authentification, ou quand l'ensemble d'ancres de confiance d'un nœud est trop faible pour qu'on puisse croire qu'il peut authentifier les homologues). De plus, les canaux sûrs qui sont susceptibles d'attaques par interposition parce que ils ne fournissent pas d'authentification de point à point utile, sont utiles quand ils sont combinés avec l'authentification de couche d'application (autrement ils sont seulement quelque chose de "mieux que rien" -- voir (BTNS, *Better Than Nothing Security*) [RFC5387]).

Par exemple, l'interface Internet de systèmes de petits ordinateurs (iSCSI, *Internet Small Computer Systems Interface*) [RFC3720] assure l'authentification de couche d'application (par exemple, en utilisant Kerberos V) mais s'appuie sur IPsec pour la protection du transport ; iSCSI ne fournit pas de lien entre les deux. Les initiateurs de iSCSI doivent veiller à s'assurer que le nom du serveur authentifié à la couche d'application et le nom de l'homologue à la couche IPsec correspondent -- une forme informelle de lien de canal.

Le présent document décrit une solution : l'utilisation du "lien de canal" pour lier l'authentification aux couches d'application aux sessions sécurisées aux couches inférieures dans la pile réseau.

1.1 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].

2. Définitions

Canal sûr : une connexion de paquets, datagrammes, flux d'octets, ou une séquence de connexions entre deux points d'extrémité qui assure l'intégrité cryptographique et, facultativement, la confidentialité des données échangées sur elle.

On suppose que le canal est sûr ; si un attaquant peut réussir, par exemple, une cryptanalyse des clés de session d'un canal, alors le canal n'est pas sûr.

Lien de canal : processus par lequel on établit qu'aucun interposé n'existe entre deux points d'extrémité qui ont été authentifiés à une couche de réseau mais utilisent un canal sûr à une couche de réseau inférieure. Ce terme est utilisé comme un nom.

Liens de canaux : [voir la note historique ci-dessous.] Généralement, certaines données qui "désignent" un canal ou un ou ses deux points d'extrémité de telle façon que si ces données peuvent être montrées, à une couche de réseau supérieure, comme étant les mêmes aux deux extrémités d'un canal, alors il n'y a pas d'interposé entre les deux points d'extrémité à cette couche de réseau supérieure. Ce terme est utilisé comme un nom.
Plus formellement, il y a deux types de liens de canaux :

+ liens de canaux uniques : liens de canaux qui désignent un canal d'une manière cryptographiquement sûre et unique dans le temps ;
+ liens de canaux de point d'extrémité : liens de canaux qui désignent les points d'extrémité authentifiés, ou même un seul point d'extrémité, d'un canal qui sont, à leur tour, liés de façon sûre au canal, mais qui n'identifient pas un canal de façon unique dans le temps.

Lien cryptographique : (par exemple, "lié cryptographiquement") opération cryptographique qui est cause qu'un objet, comme un chiffrement privé ou une clé de signature, ou un canal sûr établi, "parle pour" [Lampson91] un principal, comme un utilisateur, un ordinateur, et cœtera. Par exemple, un certificat d'infrastructure de clé publique pour certificats X.509 (PKIX, *Public Key Infrastructure for X.509 Certificates*) lie une clé privée au nom d'un principal dans le domaine de confiance du producteur de certificat de telle façon qu'un possesseur de ladite clé privée peut agir au nom de l'utilisateur (ou autre entité) désignée par le certificat. Les liens cryptographiques sont généralement de nature asymétrique (à ne pas confondre avec la cryptographie à clé symétrique ou asymétrique) en ce qu'un objet est rendu capable d'agir pour un autre, mais l'inverse n'est généralement pas le cas (on ne dit pas qu'un utilisateur parle pour ses clés privées, mais on dit que les clés privées d'un utilisateur parlent pour lui).

Noter qu'il peut y avoir de nombreuses instances de "lien cryptographique" dans une application de lien de canal. Les accréditifs qui authentifient les principaux à la couche d'application lient les clés privées ou secrètes aux identités de ces principaux, de sorte que les dites clés parlent pour eux. Un canal sûr consiste normalement en clés de session symétriques utilisées pour assurer la protection de la confidentialité et de l'intégrité au données envoyées sur le canal ; chaque clé de session d'un point d'extrémité parle pour ce point d'extrémité du canal. Finalement, chaque point d'extrémité d'un canal lié à l'authentification à la couche d'application parle pour le principal authentifié à la couche d'application sur le même côté du canal.

Les termes définis ci-dessus ont été utilisés depuis de nombreuses années et ont été pris pour signifier, au moins dans certains contextes, ce qui est déclaré ci-dessous. Malheureusement, cela signifie que "lien de canal" peut se référer au fonctionnement du lien de canal et, parfois au nom d'un canal, et "liens de canaux" -- une différence de seulement une lettre -- se réfère généralement au nom d'un canal.

Noter que le protocole d'auhentification extensible (EAP, *Extensible Authentication Protocol*) [RFC3748] utilise "lien de canal" pour se référer à une facilité qui peut paraître similaire à celle décrite ici, mais est en fait assez différente. Voir les détails au paragraphe 2.2.

2.1 Propriétés d'un lien de canal

Les applications, les cadres d'authentification (par exemple, GSS-API, SASL) les mécanismes de sécurité (par exemple, le mécanisme GSS-API de Kerberos V [RFC1964]) et les canaux sûrs doivent satisfaire les exigences et devraient suivre les recommandations mentionnées ci-dessous.

Exigences :

o Afin d'utiliser un lien de canal, les applications DOIVENT vérifier que les mêmes liens de canaux sont observés de chaque côté du canal. Pour le faire, l'application DOIT utiliser un protocole d'authentification à la couche d'application pour authentifier l'un, l'autre, ou les deux homologues de l'application (un à chaque extrémité du canal).

  * Si the protocole d'auhentification utilisé par l'application prend en charge le lien de canal, l'application DEVRAIT l'utiliser.

  * Un protocole d'authentification qui prend en charge le lien de canal DOIT fournir un créneau d'entrée dans son API pour une "bride" pour le canal, ou ses liens de canaux.

  * Si le protocole d'auhentification ne prend pas en charge le fonctionnement de lien de canal, mais fournit une "couche de sécurité" avec au moins la protection de l'intégrité, alors l'application DOIT utiliser la facilité de protection de l'intégrité du protocole d'authentification pour échanger les liens de canaux, ou leurs hachages cryptographiques.

  * Le nom du type de lien de canal DOIT être utilisé par l'application et/ou protocole d'authentification pour éviter des ambiguïtés sur les plusieurs types possibles de canaux qui sont liés. Si des instances incorporées du même type de canal sont disponibles, alors le canal le plus interne DOIT être utilisé.

- Les spécifications de liens de canaux pour tous canaux sûrs DOIVENT fournir un seul codage de chaîne d'octets en ordre canonique des liens de canaux. Dans ce cadre, les liens de canaux DOIVENT commencer par le préfixe unique de lien de canal suivi par un caractère deux-points (ASCII 0x3A).

- Les liens de canaux pour un type de canal sûr donné DOIVENT être construits d'une façon telle qu'un interposé ne pourrait pas facilement forcer les liens de canaux d'un canal donné à correspondre à ceux d'un autre.

- Les liens uniques de canaux DOIVENT lier non seulement l'échange de clé pour le canal sûr, mais aussi toutes les négociations et l'authentification qui peuvent avoir lieu pour établir le canal.

- Les liens de canaux de point d'extrémité DOIVENT être liés dans le canal sûr et toutes ses négotcations. Par exemple, une clé publique lorsque un lien de canal de point d'extrémité devrait être utilisé pour vérifier une signature de ces négociations (ou pour les chiffrer) incluant les messages de l'échange de clé initial et de négociation pour ce canal -- une telle clé va alors être liée au canal. Un nom de certificat comme lien de canal de point d'extrémité pourrait aussi être lié dans le canal d'une façon similaire, bien que dans le cas d'un nom de certificat, le lien dépende aussi de la force de l'authentification de ce nom (c'est-à-dire, la validation du certificat, les ancres de confiance, les algorithmes utilisés dans la construction et la validation du chemin de certificats, et cœtera).

- Les liens de canaux de point d'extrémité PEUVENT être des identifiants (par exemple, des noms de certificat) qui doivent être authentifiés au moyen d'une infrastructure, comme une infrastructure de clé publique (PKI, *Public Key Infrastructure*). Dans ce cas, les applications DOIVENT assurer que le canal fournit une authentification adéquate de ces identifiants (par exemple, que la politique de validation de certificat et les ancres de confiance utilisées par le canal satisfont les exigences de l'application). Pour éviter des difficultés de mise en œuvre de cette exigence, les applications DEVRAIENT utiliser des quantités cryptographiques comme liens de canaux de point d'extrémité, comme des clés publiques de sujet de certificat.

- Les applications qui désirent la protection de la confidentialité DOIVENT utiliser des services de protection de session de couche d'application pour la protection de la confidentialité quand le canal lié ne fournit pas de protection de la confidentialité.

- L'intégrité d'un canal sûr NE DOIT PAS être affaiblie si ses liens de canaux devaient être révélés à un attaquant. C'est-à-dire que la construction des liens de canaux pour tout type de canal sûr NE DOIT PAS laisser fuir d'informations secrètes sur le canal. Les liens de canaux de point d'extrémité PEUVENT cependant laisser passer des informations sur les points d'extrémité du canal (par exemple, leur nom).

- Le fonctionnement du lien de canal DOIT être au moins protégé en intégrité dans le mécanisme de sécurité utilisé à la couche d'application.

- Les cadres et mécanismes d'authentification qui prennent en charge le lien de canal DOIVENT communiquer l'échec du lien de canal aux applications.

- Les applications NE DOIVENT PAS envoyer d'informations sensibles, exigeant la protection de la confidentialité, sur le canal sous-jacent avant d'avoir achevé l'opération de lien de canal.

Recommandations :

- Les liens de canaux de point d'extrémité où les points d'extrémité sont des noms qui ont une signification NE DEVRAIENT PAS être utilisés quand le canal n'assure pas la protection de la confidentialité et que celle-ci est désirée. Autrement, les canaux qui exportent de tels liens de canaux DEVRAIENT pourvoir à l'utilisation d'un résumé et NE

DEVRAIENT PAS introduire de nouveaux problèmes d'agilité de résumé/hachage en résultant.

Options :

- Les cadres et mécanismes d'authentification qui prennent en charge le lien de canal PEUVENT échouer à établir l'authentification si le lien de canal échoue.

- Les applications PEUVENT envoyer des informations sur le canal sous-jacent et sans protection de l'intégrité de la part du protocole d'auhentification de couche d'application avant d'achever l'opération de lien de canal si de telles informations exigent seulement la protection de l'intégrité. Cela pourrait être utile pour des négociations optimistes.

- Un mécanisme de sécurité PEUT échanger des liens de canaux protégés en intégrité.

- Un mécanisme de sécurité PEUT échanger des résumés protégés en intégrité des liens de canaux. De tels mécanismes DEVRAIENT pourvoir à l'agilité de hachage/résumé.

- Un mécanisme de sécurité PEUT utiliser des liens de canaux dans l'échange de clés, l'authentification, ou la déduction de clés, avant l'échange des messages "authentifiants".

2.2. Lien de canal EAP

Ce paragraphe est pour information. Le présent document ne met pas à jour EAP [RFC3748], il n'est pas une description normative, et n'impose d'exigence sur aucun aspect de EAP ou des méthodes EAP.

EAP [RFC3748] inclut un concept de lien de canal décrit comme suit :

> "La communication au sein d'une méthode EAP de propriétés de canal protégé en intégrité telles que des identifiants de point d'extrémité qui peuvent être comparés aux valeurs communiquées via des mécanismes hors bande (comme via un protocole AAA ou de couche inférieure)."

Le paragraphe 7.15 de la [RFC3748] décrit le problème comme celui où un serveur d'accès réseau (NAS, *Network Access Server*) (autrement dit un "authentificateur") peut mentir à l'homologue (client) et lui faire prendre des décisions d'autorisation incorrectes (par exemple, sur quel trafic peut transiter à travers le NAS). Ce n'est pas tout à fait l'objet du lien de canal générique (détection d'interposé).

Le paragraphe 7.15 de la [RFC3748] appelle à un "échange protégé des propriétés du canal comme des identifiants de point d'extrémité" afin que "il soit possible de confronter les propriétés de canal fournies par l'authentificateur via des mécanismes hors bande à celles échangées au sein de la méthode EAP".

Cela a parfois été tenu pour très similaire à la notion générique de lien de canal fournie ici. Cependant, il y a une différence très subtile entre les deux concepts de lien de canal qui rend très difficile d'avancer des exigences et recommandations qui s'appliquent aux deux. La différence est sur le canal de couche inférieure :

- Dans le cas du lien de canal générique, les identités de l'une et l'autre extrémité de ce canal ne sont pertinentes pour rien d'autre que la construction d'un nom pour ce canal, et dans ce cas, les identités des points d'extrémité du canal doivent être établies à priori.

- Tandis que dans le cas d'EAP, l'identité de l'extrémité NAS du canal, et même les propriétés de sécurité du canal lui-même, peuvent être établies durant ou après l'authentification de l'homologue EAP auprès du serveur EAP.

En d'autres termes : il y a une différence fondamentale de mécanisme (moment de l'établissement du canal de couche inférieure) et dans l'objet (authentification des propriétés du canal de couche inférieure pour les besoins de l'autorisation contre détection d'interposé).

Après quelques discussions, on a conclu qu'il n'y a pas de façon simple d'obtenir des exigences et recommandations qui s'appliquent à la fois au lien de canal générique et EAP. Donc, EAP sort du domaine d'application du présent document.

3. Authentification et sémantique du lien de canal

Certains cadres et/ou mécanismes d'authentification fournissent un lien de canal, comme GSS-API et certains des mécanismes GSS-API, tandis que d'autres ne le peuvent pas, comme SASL (cependant, un travail en cours ajoute la prise en charge du lien de canal à SASL). La sémantique peut varier par rapport à la négociation, comment le lien se produit, et le traitement d'un échec du lien de canal (voir ci-dessous).

Lorsque des facilités convenables de lien de canal ne sont pas fournies, les protocoles d'application PEUVENT inclure un échange de liens de canaux séparé, protégé. Pour ce faire, le service d'authentification de couche d'application doit fournir des services de protection de message (au moins la protection de l'intégrité).

3.1 GSS-API et lien de canal

GSS-API [RFC2743] pourvoit à l'utilisation du lien de canal durant l'initialisation des contextes de sécurité de GSS-API, bien que les mécanismes GSS-API ne soient pas obligés de prendre en charge cette facilité.

Cette facilité de lien de canal est décrite dans les [RFC2743] et [RFC2744].

Les mécanismes GSS-API doivent faire échouer l'établissement du contexte de sécurité quand le lien de canal échoue, et GSS-API ne fournit pas de mécanisme pour la négociation de lien de canal. Par suite, les applications GSS-API doivent s'accorder a priori, par négociation ou autrement, sur l'utilisation du lien de canal.

Fort heureusement, il est possible de concevoir des pseudo mécanismes GSS-API qui enveloppent simplement les mécanismes existants pour permettre aux applications de négocier l'utilisation du lien de canal au sein de leurs méthodes existantes pour négocier les mécanismes GSS-API. Par exemple, NFSv4 [RFC3530] fournit sa propre négociation de mécanisme GSS-API, comme le fait le protocole SSH v2 [RFC4462]. Ces pseudo mécanismes sont proposés séparément, voir [STACKABLE].

3.2 SASL et lien de canal

SASL [RFC4422] n'assure pas encore l'utilisation de lien de canal durant l'initialisation des contextes SASL.

La [RFC5801] spécifie comment SASL, en particulier son nouveau pont vers GSS-API, effectue le lien de canal. SASL va probablement différer de GSS-API dans son traitement de l'échec de lien de canal (c'est-à-dire, quand il peut y avoir un interposé) en ce que le succès/échec de lien de canal va seulement affecter la négociation des couches de sécurité SASL. C'est-à-dire que quand le lien de canal réussit, SASL ne devrait pas choisir de couches de sécurité, laissant la protection cryptographique de la session au canal auquel l'authentification SASL a été liée.

4. Spécifications de lien de canal

Les liens de canaux pour les divers types de canaux sûrs ne sont pas décrits ici. Des spécifications de liens de canaux se trouvent dans :

Type de canal sûr	**Référence**
SSHv2	[SSH-CB]
TLS	[RFC5929]
IPsec	Il n'y a pas encore de spécification pour les liens de canaux IPsec, mais le groupe de travail IETF Sécurité mieux que rien (BTNS, *Better Than Nothing Security*) travaille à spécifier les canaux IPsec, et éventuellement les liens de canaux IPsec.

4.1 Exemples de liens de canal uniques

Le texte qui suit n'est pas normatif, mais montre comment on pourrait construire des liens de canaux pour divers types de canaux sûrs.

Pour SSHv2 [RFC4251] l'identifiant de session SSHv2 devrait suffire car il est un lien cryptographique de tous les

paramètres de connexion SSHv2 : échange et négociation de clé.

L'identifiant de session TLS [RFC4346] est simplement alloué par le serveur. À ce titre, l'identifiant de session TLS n'a pas les propriétés requises pour être utile comme lien de canal parce que tout interposé, se faisant passer pour le serveur, peut simplement allouer le même identifiant de session au client victime que le serveur a alloué à l'interposé. Les messages TLS initiaux finis non chiffrés (du client, du serveur, ou des deux) sont suffisants car ils sont le résultat de la fonction pseudo aléatoire TLS, chiffrée avec la clé de session, appliquée à tout le matériel de prise de contact.

4.2 Exemples de liens de canal de point d'extrémité

Le texte qui suit n'est pas normatff, mais est donné ici pour montrer comment on peut construire des liens de canaux pour divers types de canaux sûrs.

Pour SSHv2 [RFC4251] la clé publique d'hôte SSHv2, quand elle est présente, devrait suffire car elle est utilisée pour signer la négociation de suite d'algorithmes et l'échange de clés Diffie-Hellman; pour autant que le client respecte la clé publique d'hôte qui correspond à la clé privée d'hôte que le serveur utilise, alors il ne peut pas y avoir d'interposé dans la connexion SSHv2. Noter que tous les échanges de clé SSHv2 n'utilisent pas de clés publiques d'hôte; donc, cette construction de liens de canaux n'est pas aussi utile que celle donnée au paragraphe 4.1.

Pour TLS [RFC4346] le certificat de serveur devrait suffire pour les mêmes raisons que ci-dessus. Là encore, toutes les suites de chiffrement TLS n'impliquent pas de certificats de serveur ; donc, l'utilité de cette construction de liens de canaux est limitée aux scénarios où les certificats de serveur sont couramment utilisés.

5. Utilisation des liens de canal

Utilisations pour le lien de canal identifiées jusqu'à présent :

- Délégation de la protection cryptographique de session aux couches où le matériel peut raisonnablement être supposé prendre en charge les protocoles cryptographiques pertinents :
  - NFSv4 [RFC3530] avec placement direct des données à distance (RDDP, *Remote Direct Data Placement*) [RFC5667] pour la réception sans copie lorsque les contrôleurs d'interface réseau (NIC, *Network Interface Controller*) prennent en charge RDDP. La protection de session cryptographique va être déléguée à l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] / en-têtes d'authentification (AH, *Authentication Header*) [RFC4302].
  - iSCSI [RFC3720] avec accès direct à la mémoire distante (RDMA, *Remote Direct Memory Access*) [RFC5046]. La protection de session cryptographique va être déléguée à ESP/AH.
  - HTTP avec TLS [RFC2817] [RFC2818]. Dans les situations qui impliquent des mandataires, les utilisateurs peuvent vouloir lier l'authentification à un canal TLS entre le dernier mandataire côté client et le premier mandataire côté serveur ("le concentrateur"). Il y a un travail en cours pour étendre l'ensemble de choix d'authentification de bout en bout à la couche HTTP, qui, couplée avec le lien de canal à TLS, permetttrait des mandataires sans dégrader la protection sur les internets publics.

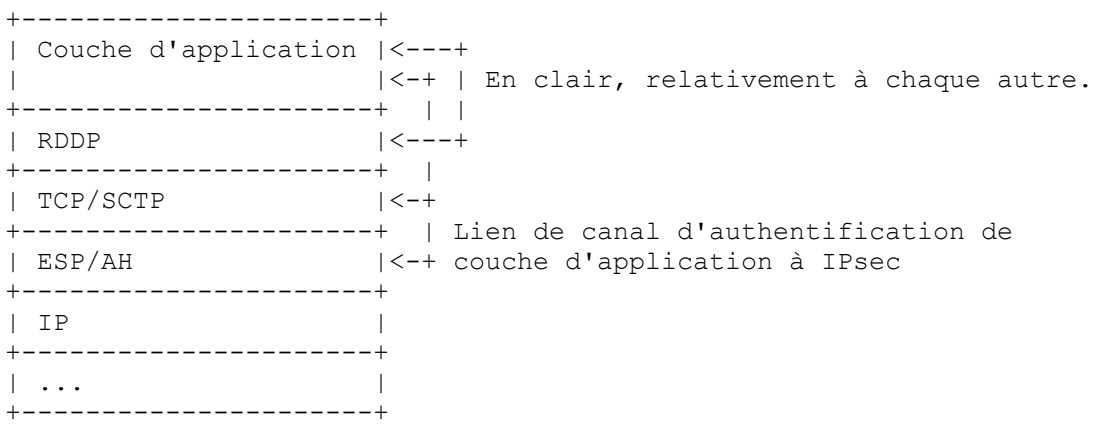
- Réduire le nombre de contextes cryptographiques actifs qu'une application doit entretenir :
  - NFSv4 [RFC3530] multiplexe plusieurs utilisateurs sur des connexions individuelles. Chaque utilisateur est authentifié séparément, et les appels de procédure distante (RPC, *Remote Procedure Call*) des utilisateurs sont protégés avec des contextes de sécurité GSS-API par utilisateur. Cela signifie que des grands clients en temps partagé doivent souvent tenir de nombreux contextes cryptographiques par connexion NFSv4. Avec le lien de canal à IPsec, ils pourraient tenir un nombre beaucoup plus petit de contextes cryptographiques par connexion NFSv4, réduisant donc la pression sur la mémoire et les interactions avec le matériel de chiffrement.

Par exemple, les applications qui souhaitent utiliser RDDP pour réaliser une réception sans copie peuvent utiliser une couche de réseau comprise par les NIC pour télécharger la livraison des données d'application dans des mémoires tampon pré-arrangées. Noter que pour obtenir une réception sans copie les données d'application doivent être en clair par rapport à cette couche RDDP, ou la mise en œuvre de RDDP doit savoir comment mettre en œuvre les protocoles de protection de session cryptographique utilisés à la couche d'application.

Il y a une multitude de protocoles de protection de session cryptographique de couche d'application disponibles. Il n'est pas raisonnable de s'attendre à ce que les NIC prennent en charge beaucoup de ces protocoles. De plus, certains protocoles

d'application peuvent tenir de nombreux contextes de session cryptographique par connexion (par exemple, NFSv4 le fait). On pense qu'il est plus simple de pousser la protection de session cryptographique à la pile réseau (à IPsec) et d'être alors capable de produire des NIC qui téléchargent d'autres opérations (c'est-à-dire, TCP/IP, ESP/AH, et DDP) que d'ajouter la prise en charge par le NIC des nombreux protocoles de protection de session cryptographique utilisés dans les applications courantes à la couche d'application.

La figure suivante montre comment les diverses couches de réseau sont en rapport :



6. Avantages du lien de canal pour sécuriser les canaux

L'utilisation de lien de canal pour déléguer la protection de session cryptographique inclut :
- o des améliorations de performances en évitant une double protection des données d'application dans le cas où IPsec est utilisé et où les applications fournissent leur propres canaux sûrs ;
- o des améliorations de performances par un effet de levier sur IPsec accéléré par le matéiel ;
- o des améliorations de performances en permettant au téléchargement de matériel RDDP d'être intégré à l'accélération de matériel IPsec. Lorsque les protocoles mis en couche au dessus de RDDP utilisent la protection de la confidentialité, le téléchargement RDDP ne peut pas être fait. Donc, en utilisant le lien de canal à IPsec, la protection de la confidentialité est déplacée à IPsec, qui est mis en couche en dessous de RDDP. Donc, RDDP peut traiter les données de protocole d'application qui sont en clair par rapport aux en-têtes RDDP.
- o Des améliorations de la latence pour les applications qui multiplexent plusieurs utilisateurs sur un seul canal, comme NFS avec RPCSEC_GSS [RFC2203].

La délégation de la protection de session cryptographique à IPsec exige des caractéristiques non encore spécifiées. Il y a des travaux en cours pour spécifier :
- o les canaux IPsec [RFC5660] ;
- o les interfaces de programmation d'application (API) relatives aux canaux IPsec [BTNS-IPSEC] ;
- o les liens de canaux pour les canaux IPsec ;
- o l'authentification faible d'infrastructure IPsec [RFC5386].

7. Considérations relatives à l'IANA

L'IANA a créé un nouveau registre pour les spécifications de liens de canaux pour divers types de canaux.

L'objet de ce registre est non seulement d'assurer l'unicité des valeurs utilisées pour nommer les liens de canaux, mais aussi de fournir une référence définitive aux spécifications techniques détaillant chaque lien de canal disponible à utiliser sur l'Internet.

Il n'y a pas de convention de dénomination pour les liens de canaux : toute chaîne composée de caractères US-ASCII alphanumériques, point ('.'), et tiret ('-') suffira.

La procédure détaillée au paragraphe 7.1 est à utiliser pour l'enregistrement d'une valeur désignant un mécanisme individuel spécifique.

7.1 Procédure d'enregistrement

L'enregistrement d'un nouveau lien de canal requiert une revue par un expert comme défini dans le BCP 26 [RFC2434].

L'enregistrement d'un lien de canal est demandé en remplissant le gabarit suivant :

Sujet : Enregistrement du lien de canal X
Préfixe unique de lien de canal (nom) :
Type de lien de canal : ("unique" ou "point d'extrémité")
Type de canal : (par exemple, TLS, IPsec, SSH, etc.)
Spécification publiée (recommandé, facultatif) :
Le lien de canal est secret (exige la protection de la confidentialité) : oui/non
- Description (facultatif si une spécification est donnée ; exigé si aucune spécification publiée n'est spécifiée) :
- Usage prévu : (COMMUN, USAGE LIMITÉ, ou OBSOLÈTE)
- Adresse et messagerie de la personne à contacter pour pluus d'informations :
- Nom du propriétaire/contrôleur des changements et adresse de messagerie électronique :
- Nom de l'expert réviseur et informations de contact : (laisser en blanc)
- Note : (Toutes les autres informations que l'auteur estime pertinentes peuvent être ajoutées ici.)

et en l'envoyant via messsagerie électronique à <channel-binding@ietf.org> (une liste de diffusion publique) et avec copie à l'IANA à <iana@iana.org>.

Après un délai de deux semaines pour les apports de la communauté sur la liste de diffusion, un expert va déterminer la suite à donner à la demande d'enregistrement et approuver ou désapprouver la demande avec ses justifications au demandeur, à la liste de diffusion, et à l'IANA.

Si l'expert approuve l'enregistrement, il ajoute son nom à la soumission d'enregistrement.

L'expert a la principale responsabilité de s'assurer que les liens de canaux pour les spécifications de l'IETF passent par le processus de consensus de l'IETF et que les préfixes sont uniques.

La revue devrait se concentrer sur la convenance du lien de canal demandé pour l'utilisation proposée, l'à propos du préfixe proposé, et la correctionn du type de lien de canal dans l'enregistrement. La portée de cette revue de demande peut prendre en considération les aspects pertinents de toute spécification technique fournie, comme la section des considérations relatives à l'IANA. Cependant, cette revue se concentre sur le caractère approprié de l'enregistrement demandé et non sur la pertinence des spécifications techniques fournies.

Les auteurs sont invités à poursuivre la revue par la communauté en envoyant la spécification technique comme projet Internet et en sollicitant des commentaires sur les listes de diffusion appropriées de l'IETF.

7.2 Commentaires sur les enregistrements de liens de canal

Les commentaires sur les liens de canaux enregistrés devraient d'abord être envoyés au "propriétaire" des liens de canaux et à la liste de diffusion du lien de canal.

Les auteurs de commentaires peuvent, après une tentative raisonnable de contact du propriétaire, demander à l'IANA de joindre leur commentaire à l'enregistrement de type de lien de canal lui-même en envoyant un message à <iana@iana.org>. À la seule discrétion de l'IANA, le commentaire peut être joint à l'enregistrement des liens de canaux.

7.3 Contrôle des changements

Une fois que l'enregistrement des liens de canaux a été publié par l'IANA, l'auteur peut demander un changement de sa définition. La demande de changement suit la même procedure que la demande d'enregistrement.

Le propriétaire de liens de canaux peut passer la responsabilité des liens de canaux à une autre personne ou agence en en informant l'IANA ; cela peut être fait sans discussion ni revue.

L'IESG peut réallouer la responsabilité de l'enregistrement de liens de canaux. Le cas le plus courant va être pour permettre

de faire des changemens à des mécanismes lorsque l'auteur de l'enregistrement est décédé, ne peut pas être contacté, ou est autrement incapable de faire des changements qui sont importants pour la communauté.

Les enregistrements de liens de canaux ne peuvent pas être supprimés ; les mécanismes dont l'utilisation est estimée n'être plus appropriée peuvent être déclarés OBSOLÈTES par un changement de leur champ "Utilisation prévue". De tels liens de canaux seront clairement marqués dans les listes publiées par l'IANA.

L'IESG est considéré être le propriétaire de tous les liens de canaux qui sont sur la voie de la normalisation de l'IETF.

8. Considérations sur la sécurité

Les considérations sur la sécurité apparaissent tout au long du présent document. Voir en particulier le paragraphe 2.1.

Quand on délègue la protection de session d'une couche à une autre, on va presque certainement faire des compromis sur la sécurité de session, comme d'utiliser des modes de chiffrement plus faibles dans une couche que ce qui pourrait être utilisé dans l'autre. L'évaluation et la comparaison de la force cryptographique relative de ces modes de chiffrement est difficile, ne peut pas être facilement automatisée, et sort du domaisne d'application de ce document. Les développeurs et administrateurs devraient comprendre ces compromis. Les cadres et mécanismes d'authentification d'interfaces de canaux sûrs et de couche d'application pourraient fournir des notions de profil de sécurité afin que les applications puissent éviter de déléguer la protection de session à des canaux qui sont trop faibles pour satisfaire aux exigences d'un profil de sécurité.

Le lien de canal rend utiles les canaux "anonymes" (où ni l'un ni l'autre des points d'extrémité n'est authentifié fortement à l'autre). Les mises en œuvre devraient éviter de rendre facile l'utilisation de tels canaux sans un lien de canal.

La sécurité d'un lien de canal dépend de la sécurité des canaux, de la construction de leurs liens de canaux, et de la sécurité du mécanisme d'authentification utilisé par l'application et de sa méthode de lien de canal.

Les liens de canaux devraient être construits d'une façon telle que révéler les liens de canaux d'un canal à des tiers n'affaiblisse pas la sécurité du canal. Cependant, pour la découverte des liens de canaux de point d'extrémité les liens de canaux peuvent divulguer l'identité des homologues.

8.1 Liens de canal non uniques et rétablissement de lien de canal

Les développeurs d'applications peuvent être tentés d'utiliser des liens de canaux non uniques pour une réauthentification rapide à la suite d'un rétablissement de canal. Il faut veiller à éviter la possibilité d'attaques sur les systèmes multi utilisateurs.

Considérons un protocole de multiplexage d'utilisateurs comme NFSv4 qui utilise un lien de canal à IPsec sur un client multi-utilisateurs. Si un autre utilisateur peut se connecter directement à l'accès 2049 (NFS) sur un serveur qui utilise IPsec et affirme simplement des brides d'accrédirifs RPCSEC_GSS, alors cet utilisateur va être capable de se faire passer pour tout utilisateur authentifié par le client auprès du serveur. C'est parce que la nouvelle connexion va avoir les mêmes liens de canaux que le client NFS ! Pour empêcher cela, le serveur doit exiger qu'au moins un principal de client fondé sur l'hôte, et peut-être tous les principaux d'utilisateur du client, se réauthentifie et effectue le lien de canal avant que le serveur permette aux clients d'affirmer les brides de contexte RPCSEC_GSS. Autrement, le protocole pourrait exiger a) que des canaux sûrs fournissent la protection de la confidentialité et b) que les mouchards de réauthentification rapide soient difficiles à deviner (par exemple, de grands nombres choisis au hasard).

Dans d'autres contextes, il peut ne pas y avoir de tels problèmes, par exemple, dans le cas de protocoles d'application qui ne multiplexent pas d'utilisateurs sur un seul canal et où la protection de la confidentialité est toujours utilisée dans le canal sûr.

9. Références

9.1 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)

9.2 Références pour information

[BTNS-IPSEC] Richardson, M. and B. Sommerfeld, "Requirements for an IPsec API", Travail en cours, avril 2006.

[Lampson91] Lampson, B., Abadi, M., Burrows, M., and E. Wobber, "Authentication in Distributed Systems: Theory and Practice", octobre 1991.

[RFC1964] J. Linn, "Mécanisme GSS-API de Kerberos version 5", juin 1996. (*MàJ par* RFC4121 et RFC6649)

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

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC2743] J. Linn, "Interface générique de programme d'application de service de sécurité, version 2, mise à jour 1", janvier 2000. (*MàJ par* RFC5554)

[RFC2744] J. Wray, "API de service générique de sécurité, version 2 : liaisons C", janvier 2000. *(P.S.)*

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

[RFC2818] E. Rescorla, "HTTP sur TLS", mai 2000. *(Information ; remplacée par* RFC9110*)*

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

[RFC3720] J. Satran et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI)", avril 2004. *(Remplacée par* RFC7143)

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

[RFC4120] C. Neuman et autres, "Service Kerberos d'authentification de réseau (V5)", juillet 2005. (*MàJ par* RFC4537, 5021, 6649, 7751, 8062, 8129, 8429)

[RFC4251] T. Ylonen et C. Lonvick, "Architecture du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(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)

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

[RFC4462] J. Hutzelman et autres, "Authentification et échange de clés d'interface de programme d'application de service de sécurité générique (GSS-API) pour le protocole Secure Shell (SSH)", mai 2006. *(P.S. ; MàJ par RFC8732,* 9142*)*

[RFC5046] M. Ko et autres, "Extensions pour l'accès direct à une mémoire distante (RDMA) à l'interface système de petit ordinateur à l'Internet (iSCSI)", octobre 2007. *(P.S. ; Remplacée par* RFC7145)

[RFC5386] N. Williams, M. Richardson, "La sécurité mieux que rien : un mode non authentifié de IPsec", novembre 2008. *(P.S.)*

[RFC5387] J. Touch et autres, "Problème et déclaration d'applicabilité pour la sécurité mieux que rien (BTNS)", novembre 2008. *(Info.)*

[RFC5660] N. Williams, "Canaux IPsec : verrouillage de connexion**",** octobre 2009. *(P.S.)*

[RFC5667] T. Talpey, B. Callaghan, "Placement des données directes dans le système de fichiers réseau (NFS)", janvier 2010. *(P.S. ; remplacée par* RFC8267)

[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*)*

[RFC5929] J. Altman, N. Williams, L. Zhu, "Liaisons de canaux pour TLS", juillet 2010. *(P. S. ; MàJ par* RFC9266*)*

[SSH-CB] Williams, N., "Channel Binding Identifiers for Secure Shell Channels", Travail en cours, novembre 2007.

[STACKABLE] Williams, N., "Stackable Generic Security Service Pseudo-Mechanisms", Travail en cours, juin 2006.

Appendice A. Remerciements

Merci à Mike Eisler pour son travail sur le document du mécanisme de conjonction de canal et pour avoir trouvé la solution du problème, à Sam Hartman pour avoir souligné que le lien de canal apporte une solution générale au problème du lien de canal, et à Jeff Altman pour sa suggestion d'utiliser les messages TLS finis comme liens de canal TLS. Merci aussi à Bill Sommerfeld, Radia Perlman, Simon Josefsson, Joe Salowey, Eric Rescorla, Michael Richardson, Bernard Aboba, Tom Petch, Mark Brown, et de nombreux autres.

Adresse de l'auteur

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct.
Austin, TX 78727
US

mél : Nicolas.Williams@sun.com

Déclaration complète de droits de reproduction

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 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.