Groupe de travail Réseau
Request for Comments : 3897
Catégorie : Information
Traduction Claude Brière de L'Isle

A. Barbir, Nortel Networks

septembre 2004

Communication des entités et des points d'extrémité des services marginaux à connexion libre (OPES)

Statut de ce mémoire
Le présent document apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de normes de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire documente les exigences de traçage et de non blocage (outrepassement) pour les services marginaux à connexion libre (OPES, *Open Pluggable Edge Services*).

Table des matières

1. Introduction

L'architecture pour les services marginaux à connexion libre (OPES) [RFC3835] permet des services d'application coopératifs (services OPES) entre un fournisseur de données, un consommateur de données, et zéro, un ou plusieurs processeurs OPES. Les services d'application considérés analysent et éventuellement transforment les messages de niveau application échangés entre le fournisseur et le consommateur des données.

Ce travail spécifie les fonctionnalités de traçage et d'outrepassement des OPES. Le document d'architecture [RFC3835] exige que le traçage soit pris en charge dans la bande. Cet objectif de conception limite le type des protocoles d'application que les OPES peuvent prendre en charge. Les détails de ce qu'un enregistrement de trace peut porter dépend aussi des choix du

protocole de niveau application. Pour ces raisons, le présent travail ne documente que les exigences pour les entités OPES qui sont nécessaires à la prise en charge des fonctions de traçage et d'outrepassement. La tâche du codage des caractéristiques de traçage et d'outrepassement est spécifique du protocole d'application. Des documents distincts vont traiter de HTTP et des autres protocoles.

L'architecture n'empêche pas de développer des protocoles et des techniques hors bande pour traiter le traçage et l'outrepassement. De tels protocoles sortent du domaine d'application du présent travail.

1.1 Terminologie

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]. Lorsque utilisés avec des significations normatives, ces mots-clés seront tout en majuscules. Les occurrences de ces mots en minuscules conservent leur utilisation en prose normale, sans implication normative.

2. Le système des OPES

Cette section donne une définition du système des OPES. Ceci est nécessaire afin de définir ce qui est traçable (ou outrepassable) dans un flux d'OPES.

Définition : un système OPES est un ensemble de toutes les entités OPES autorisées, par le fournisseur des données ou par l'application de consommateur des données, à traiter un certain message d'application.

La nature de l'accord d'autorisation détermine si la délégation d'autorité est transitive (ce qui signifie qu'une entité autorisée est autorisée à inclure d'autres entités).

Si des accords d'autorité spécifiques permettent la re-délégation, un système OPES peut être formé par induction. Dans ce cas, un système OPES commence avec des entités directement autorisées par une application de fournisseur de données (ou de consommateur de données). Le système OPES inclut alors toute entité OPES autorisée par une entité qui est déjà dans le système OPES. La délégation d'autorité est toujours vue dans le contexte d'un certain message d'application.

Un système OPES se définit message d'application par message d'application. Avoir l'autorité pour traiter un message n'implique pas d'être impliqué dans le traitement du message. Donc, certains membres de système OPES peuvent ne pas participer au traitement d'un message. De même, certains membres peuvent traiter plusieurs fois le même message.

La définition ci-dessus implique qu'il ne peut pas y avoir plus de deux systèmes OPES (les systèmes OPES côté client et côté serveur peuvent traiter le même message en même temps) qui traitent le même message à un certain moment. Ceci se fonde sur l'hypothèse qu'il y a un seul fournisseur de données et un seul consommateur de données pour ce qui concerne un certain message d'application.

Par exemple, considérons un réseau de livraison de contenu (CDN, *Content Delivery Network*) qui livre une image au nom d'un site de la Toile occupé. Les processeurs et services OPES, que le CDN utilise pour adapter et livrer l'image, comportent un système OPES. Dans un exemple plus complexe, un système OPES contiendrait des entités OPES tierces que le CDN engage pour effectuer les adaptations (par exemple, pour ajuster la qualité de l'image).

3. Exigences pour le traçage

On donne ensuite la définition de la trace et du traçage OPES.

Trace OPES : informations de message d'application sur des entités OPES qui ont adapté le message.

Traçage OPES : processus de création, manipulation, ou interprétation d'une trace OPES.

Noter que la définition de la trace ci-dessus suppose un traçage dans la bande. Cette dépendance peut être supprimée si on le désire. Le traçage est effectué message par message. Le format de la trace dépend du protocole d'application qui est adapté. Une entité traçable peut apparaître plusieurs fois dans une trace (par exemple, chaque fois qu'elle agit sur un message).

3.1 Entités traçables

Ce paragraphe se concentre sur l'identification des entités traçables dans un flux OPES.

Les informations de traçage fournissent une "extrémité" avec les informations sur les entités OPES qui ont adapté les données. Il y a deux utilisations distinctes des traces OPES. D'abord, une trace permet à une "extrémité" de détecter la présence du système OPES. Une telle "extrémité" devrait être capable de voir une entrée de trace, mais n'a pas besoin d'être capable de l'interpréter au delà de l'identification du système OPES et de la localisation de certaines divulgations requises exigées par OPES (voir au paragraphe 3.2).

Ensuite, l'administrateur du système OPES est supposé être capable d'interpréter le contenu d'une trace OPES. La trace peut être relayée à l'administrateur par une "extrémité" sans interprétation, comme des données opaques (par exemple, un paquet TCP ou une photographie de message HTTP). L'administrateur peut utiliser les informations de trace pour identifier les entités OPES participantes. L'administrateur peut utiliser la trace pour identifier les services d'adaptation appliqués ainsi que d'autres informations spécifiques du message.

Comme les administrateurs des divers systèmes OPES peuvent avoir des façons diverses de chercher dans le traçage, ils doivent être libres de ce qu'ils mettent dans les enregistrements de trace et de la façon dont ils les formatent.

Au niveau de la mise en œuvre, pour une certaine trace, une entité OPES impliquée dans le traitement du message d'application correspondant est traçable ou tracée si les informations sur elle apparaissent dans cette trace. Le présent document ne spécifie aucun ordre pour ces informations. L'ordre des informations dans une trace peut être spécifique du système OPES ou peut être défini par les documents qui lient les applications.

Les entités OPES ont différent niveaux d'exigence de traçabilité. Précisément,
- o Un système OPES DOIT ajouter son entrée à la trace.
- o Un processeur OPES DEVRAIT ajouter son entrée à la trace.
- o Un service OPES PEUT ajouter son entrée à la trace.
- o Une entité OPES PEUT déléguer l'ajout de son entrée de trace à une autre entité OPES. Par exemple, un système OPES peut avoir un processeur OPES dédié pour ajouter des entrées système ; un processeur OPES peut utiliser un service d'invocation pour gérer toutes les manipulations de trace OPES (car de telles manipulations sont des adaptations OPES).

Dans un contexte OPES, une bonne approche du traçage est similaire à un ticket trouble prêt pour un abonnement à une adresse connue. L'adresse est imprimée sur le ticket. La trace en elle-même n'est pas nécessairement une description détaillée de ce qui s'est passé. Il est de la responsabilité de l'opérateur de décoder les détails de la trace et de résoudre les problèmes.

3.2 Exigences du système

Les exigences suivantes précisent les actions lors de la formation d'une entrée de trace de système OPES :
- o le système OPES DOIT inclure son identification univoque dans l'entrée de trace. Ici, l'unicité de la portée est tous les systèmes OPES qui peuvent adapter le message tracé.
- o Un système OPES DOIT définir son impact sur la validité de référence inter et intra document.
- o Un système OPES DOIT inclure des informations sur sa politique de confidentialité, incluant l'identité de la partie responsable de l'établissement et de l'application de la politique.
- o Un système OPES DEVRAIT inclure des informations qui identifient, pour le contact technique, les processeurs OPES impliqués dans le traitement du message.
- o Lorsque il fournit les informations requises, un système OPES PEUT utiliser un seul URI pour identifier une ressource contenant plusieurs éléments requis. Par exemple, un système OPES peut pointer sur une seule page de la Toile avec une référence à la politique de confidentialité du système et les informations de contact technique.

La présente spécification ne définit pas la signification des termes "politique de confidentialité, "application de politique", ou "validité de référence" ni "contact technique" et ne contient pas d'exigence concernant le codage, langage, format, ou tout autre aspect de ces informations. Par exemple, un URI utilisé pour une entrée de trace de système OPES peut ressembler à "http://www.examplecompany.com/opes/?client=example.com" où la page de la Toile identifiée est générée de façon dynamique et contient la totalité des informations de système OPES exigées ci-dessus.

3.3 Exigences pour le processeur

Les exigences suivantes précisent quand former une entrée de trace de système OPES :
- o le processeur OPES DEVRAIT ajouter son identification univoque à la trace. Ici, l'unicité de la portée est le système OPES contenant le processeur.

3.4 Exigences pour le serveur d'invocation

Dans un système OPES, c'est la tâche d'un processeur OPES d'ajouter les enregistrements de trace aux messages d'application. L'administrateur du système OPES décide si et sous quelles conditions les serveurs d'invocation peuvent ajouter des informations de trace aux messages d'application.

4. Exigences pour l'outrepassement (dispositif de non blocage)

La recommandation (3.3) de l'IAB [RFC3238] exige que l'architecture OPES n'empêche pas une application de consommateur de données de restituer une version non OPES du contenu à partir d'une application de fournisseur de données, pourvu que le contenu non OPES existe. La recommandation (3.3) de l'IAB suggère que le dispositif de non blocage (outrepassement) soit utilisé pour outrepasser les intermédiaires OPES fautifs (une fois qu'ils ont été identifiés, par une méthode quelconque).

Pour répondre à la considération (3.3) de l'IAB, on doit spécifier ce qui constitue un contenu non OPES. Dans le présent document, la définition d'un contenu "non OPES" dépend du fournisseur. Dans certains cas, la disponibilité d'un contenu "non OPES" peut être fonction de la politique interne d'une certaine organisation qui a souscrit les services d'un fournisseur OPES. Par exemple, la Compagnie A a un contrat avec un fournisseur OPES pour effectuer une recherche de virus sur toutes les pièces jointes de messagerie électronique. Un employé X de la Compagnie A peut produire une demande non bloquante au service d'examen des virus. La demande pourra être ignorée par le fournisseur OPES car elle est en contradiction avec son accord avec la Compagnie A.

La disponibilité de contenus non OPES peut être une fonction des politiques des fournisseurs de contenu (ou des consommateurs, ou des deux) et des scénarios de déploiement [RFC3752]. Pour cette raison, le présent document ne tente pas de définir ce qu'est un contenu OPES par opposition à un contenu non OPES. La signification d'un contenu OPES par rapport à un contenu non OPES est supposée être déterminée à travers les divers accords entre le fournisseur OPES, et le fournisseur et/ou consommateur des données. L'accord détermine quels services OPES peuvent être outrepassés et dans quel ordre (si c'est applicable).

La présente spécification précise l'outrepassement d'un service ou d'un groupe de services OPES identifié par un URI. Dans ce contexte, "outrepasser le service" pour un certain message d'application dans un flux OPES signifie "ne pas invoquer le service" pour ce message d'application. Un URI d'outrepassement qui identifie un système OPES (processeur) correspond à tous les services rattachés à ce système OPES (processeur). Cependant, l'outrepassement des processeurs OPES et des systèmes OPES eux-mêmes exige des mécanismes non OPES et sort du domaine d'application de la présente spécification. Un outrepassement demande une instruction d'outrepasser, généralement incorporée dans un message d'application.

La spécification actuelle ne fournit pas de bon mécanisme qui permette à une "extrémité" de spécifier "d'outrepasser ce service mais seulement si il fait partie de ce système OPES" ou "d'outrepasser tous les services de ce système OPES mais pas de ce système OPES". De plus, si un processeur OPES ne sait pas avec certitude qu'un URI d'outrepassement ne correspond pas à son service, il doit sauter ce service.

Si aucun contenu non OPES n'est disponible sans le service spécifié, la demande d'outrepassement pour ce service doit être ignorée. Ce concept implique qu'il peut être impossible de détecter l'existence de contenu non OPES ou de détecter des violations des règles d'outrepassement dans des environnements où le vérificateur ne sait pas si il existe des contenus non OPES. Ce concept suppose que la plupart des demandes d'outrepassement sont destinées à des situations où servir un contenu OPES indésirable OPES est préférable à servir un message d'erreur qu'aucun contenu non OPES préféré n'existe.

La caractéristique outrepassement est aux services OPES qui fonctionnent mal comme la demande HTTP "reload" est aux antémémoires HTTP qui fonctionnent mal. Le principal objet de l'outrepassement est d'obtenir le contenu utilisable en présence de défaillances de service et non de fournir au consommateur de contenu plus d'informations sur ce qui est en train de se passer. La trace OPES devrait être utilisée plutôt pour cet objet principal.

Bien que le présent document définisse une caractéristique de "service d'outrepassement si possible", il y a d'autres caractéristiques d'outrepassement en rapport qui peuvent être mises en œuvre dans OPES et/ou dans les protocoles d'application qui sont adaptés. Par exemple, "outrepasser le service ou générer une erreur" ou "outrepasser l'entité OPES ou générer une erreur". De tels services seraient utiles pour déboguer les systèmes OPES cassés et peut être défini dans d'autres spécifications OPES. Le présent document se concentre sur la documentation d'une caractéristique d'outrepassement au niveau de l'utilisateur répondant directement aux soucis de l'IAB.

4.1 Entités outrepassables

Dans le présent document, l'accent est mis sur le développement d'une caractéristique d'outrepassement qui permette à un utilisateur d'ordonner au système OPES d'outrepasser certains de, ou tous ses services. La collection des services OPES qui

peuvent être outrepassés est fonction de l'accord du fournisseur OPES avec soit l'application de fournisseur de contenu, soit l'application de consommateur de contenu, soit les deux. En général, une demande d'outrepassement est vue comme une instruction d'outrepassement contenant un URI qui identifie une entité OPES ou un groupe d'entités OPES qui effectue un service (ou des services) à outrepasser. Une instruction peut contenir plus d'un de ces URI. Un identifiant spécial à caractère générique peut être utilisé pour représenter tous les URI possibles.

Dans un flux OPES, une demande d'outrepassement est traitée par chaque processeur OPES impliqué. Cela signifie qu'un processeur OPES examine l'instruction d'outrepassement et si un contenu non OPES est disponible, le processeur saute alors les services indiqués. La demande est alors transmise au prochain processeur OPES dans le flux OPES. Le prochain processeur OPES va alors traiter toutes les demandes d'outrepassement, sans considération des prochaines actions du processeur. La chaîne de traitement se continue tout le long des processeurs qui sont impliqués dans le flux OPES.

4.2 Exigences pour le système

Dans un système OPES, les demandes d'outrepassement sont généralement "client centriques" (générées par l'application de consommateur de données) et vont dans la direction opposée des demandes de traçage. Le présent document demande que la caractéristique d'outrepassement soit effectuée dans la bande comme une extension à un protocole spécifique d'application. Les entités non OPES devraient être capables d'ignorer ces extensions en toute sécurité. Le présent document n'empêche pas les systèmes OPES de développer leurs propres protocoles hors bande.

Les exigences suivantes s'appliquent au dispositif d'outrepassement relatif à un système OPES (la disponibilité d'un contenu non OPES est une précondition) :

- un système OPES DOIT prendre en charge un dispositif d'outrepassement ; cela signifie que le système OPES outrepasse les services dont les URI sont identifiés par une "extrémité" OPES ;
- un système OPES DOIT fournit la version OPES du contenu si une version non OPES n'est pas disponible.

Afin de faciliter le débogage (ou le ressenti de l'utilisateur consommateur de données) du dispositif d'outrepassement dans un système OPES, il serait avantageux que les entités non outrepassées incluent des informations relatives aux raisons pour lesquelles elles ont ignoré l'instruction d'outrepassement. Il est important de noter que dans certains cas, le dispositif de traçage lui-même peut être cassé et tout le système OPES (ou une partie) peut devoir être outrepassé par la production d'une instruction d'outrepassement.

4.3 Exigences pour le processeur

Les exigences d'outrepassement (la disponibilité d'un contenu non OPES est une pré condition) pour les processeurs OPES sont :

- Le processeur OPES DEVRAIT être capable d'interpréter et traiter une instruction d'outrepassement. Cette exigence s'applique à toutes les instructions d'outrepassement, incluant celles qui identifient des services d'inconnu à receveur.
- Les processeurs OPES DOIVENT transmettre la demande d'outrepassement au prochain bond d'application pourvu que le prochain bond comprenne le protocole d'application avec la prise en charge de l'outrepassement OPES.
- Le processeur OPES DEVRAIT être capable d'outrepasser l'exécution de son ou ses services.

Les processeurs OPES qui savent comment traiter et interpréter une instruction d'outrepassement ont les exigences suivantes :

- Le receveur d'une instruction d'outrepassement avec un URI qui n'identifie aucune entité OPES connue du receveur DOIT traiter cet URI comme un identifiant à caractère générique (signifiant d'outrepasser tous les services applicables).

4.4 Exigences pour le serveur d'invocation

Dans un système OPES, il appartient à un processeur OPES de traiter les demandes d'outrepassement. L'administrateur du système OPES décide si, et sous quelles conditions, les serveurs d'invocation traitent les demandes d'outrepassement.

5. Liens de protocole

Les tâches de codage des dispositifs de traçage et d'outrepassement sont spécifiques du protocole d'application. Des documents séparés vont s'occuper de HTTP et des autres protocoles. Ces documents vont traiter de l'ordre des informations de trace comme nécessaire.

6. Considérations de conformité

La présente spécification définit la conformité pour les sujets de conformité suivants : système OPES, processeurs, entités et serveurs d'invocation.

Un sujet de conformité est conforme si il satisfait à toutes les exigences de niveau "DOIT" et "DEVRAIT" applicables. Par définition, satisfaire une exigence de niveau "DOIT" signifie agir comme prescrit par l'exigence ; satisfaire à une exigence de niveau "DEVRAIT" signifie soit agir comme prescrit par l'exigence, soit avoir une raison d'agir différemment. Une exigence est applicable au sujet si elle donne des instructions au sujet.

De façon informelle, la conformité au présent document signifie qu'il n'y a pas de violations connues des "DOIT" et que toutes les violations des "DEVRAIT" sont conscientes. En d'autres termes, un "DEVRAIT" signifie "DOIT satisfaire ou DOIT avoir une raison de violer". On s'attend à ce que les revendications de conformité soient accompagnées d'une liste de DEVRAIENT non pris en charge (si il en est) dans un format approprié, expliquant pourquoi le comportement préféré n'a pas été choisi.

Seules les parties normatives de la présente spécification affectent la conformité. Les parties normatives sont : les parties explicitement marquées en utilisant le mot "normatif", les définitions, et les phrases contenant des mots en majuscules non entre guillemets provenant de la [RFC2119]. Par conséquent, les exemples et illustrations ne sont pas normatifs.

7. Considérations relatives à l'IANA

La présente spécification ne contient pas de considérations relatives à l'IANA. Les liens d'application PEUVENT contenir des considérations relatives à l'IANA spécifiques de l'application.

8. Considérations sur la sécurité

Les considérations sur la sécurité des OPES sont documentées dans la [RFC3837]. Les questions de politique et d'autorisation sont traitées dans la [RFC3838]. Il est recommandé que les concepteurs consultent ces documents avant de lire cette section.

Le présent document est un document sur les exigences pour les caractéristiques de traçage et d'outrepassement. Les exigences qui sont établies dans le présent document peuvent être utilisées pour étendre un protocole de niveau application à prendre en charge ces caractéristiques. À ce titre, ce travail exige quelques précautions pour la sécurité.

8.1 Considérations sur la sécurité du traçage

La facilité de traçage pour l'architecture OPES est mise en œuvre comme une extension de protocole. Des mises en œuvre inadéquates de la facilité de traçage peuvent déjouer les sauvegardes introduites dans l'architecture OPES. La facilité de traçage par elle-même peut devenir une cible d'attaques malveillantes ou être utilisée pour lancer des attaques contre un système OPES.

Les menaces causées par, ou contre la facilité de traçage peuvent être vues comme des menaces au niveau application dans un flux OPES. Dans ce cas, les menaces peuvent affecter le consommateur de données et l'application de fournisseur des données.

Comme les informations de traçage sont une extension de protocole, ces traces peuvent être injectées dans le flux de données par des entités non OPES. Dans ce cas, il y a des risques que des entités non OPES puissent être compromises d'une façon qui menace l'intégrité et l'efficacité globales d'un système OPES. Par exemple, un mandataire non OPES peut ajouter de fausses informations de traçage dans une trace. Cela peut être fait sous la forme de mauvais services, ou indésirables, ou non existants. Une entité non OPES peut injecter des traces de grande taille qui peuvent causer un débordement de mémoire tampon dans une application de consommateur des données. Les mêmes menaces peuvent apparaître à partir d'entités OPES compromises. Un attaquant peut contrôler une entité OPES et injecter de mauvaises, ou très grosses, informations de trace qui peuvent submerger une extrémité ou la prochaine entité OPES dans un flux OPES. Des menaces similaires peuvent résulter de mauvaises mises en œuvre de la facilité de traçage dans des entités OPES de confiance.

Des informations de traçage compromises peuvent être utilisées pour lancer des attaques sur un système OPES qui donnent l'impression qu'une transformation involontaire a été effectuée sur les données. Cela peut être réalisé en insérant un faux identifiant d'entité (un processeur OPES). Une trace compromise peut affecter l'intégrité de la structure globale du message. Cela peut affecter des entités qui utilisent les informations d'en-tête de message pour effectuer des services comme la comptabilité, l'équilibrage de charge ou des services fondés sur la référence.

Les informations de trace compromises peuvent être utilisées pour lancer des attaques de déni de service qui peuvent submerger une application de consommateur de données ou une entité OPES dans un flux OPES. Insérer de fausses informations de traçage peut compliquer les tâches de débogage effectuées par l'administrateur de système durant les réparations de troubles du comportement du système OPES.

À titre de précaution, les entités OPES devraient être capables de vérifier que les traces insérées sont effectuées par des entités OPES légales. Cela peut être fait au titre des activités d'autorisation et d'authentification. La politique peut être utilisée pour indiquer quelles informations de trace peuvent être attendues d'une entité homologue. Les autres questions de sécurité relatives au niveau application se trouvent dans la [RFC3837].

8.2 Considérations sur la sécurité de l'outrepassement

La facilité d'outrepassement pour l'architecture OPES est mise en œuvre comme une extension de protocole. Les mises en œuvre inadéquates de la facilité d'outrepassement peuvent déjouer les sauvegardes construites dans l'architecture OPES. La facilité d'outrepassement par elle-même peut devenir une cible d'attaques malveillantes ou utilisée pour lancer des attaques contre un système OPES.

Les menaces causées par, ou contre la facilité d'outrepassement peuvent être vues comme des menaces au niveau de l'application dans un flux OPES. Dans ce cas, les menaces peuvent affecter l'application du consommateur de données et du fournisseur de données.

Il y a des risques pour le système OPES par des entités non OPES, par lesquels ces entités peuvent insérer des instructions d'outrepassement dans le flux OPES. La menace peut venir d'entités non OPES compromises. La menace peut affecter l'intégrité globale et l'efficacité d'un système OPES. Par exemple, un mandataire non OPES peut ajouter une instruction d'outrepassement aux entités OPES légitimes. L'attaque peut résulter en une surcharge des serveurs fournisseurs de contenu original, car l'attaque court-circuite toutes les techniques d'équilibrage de charge. De plus, une telle attaque est aussi équivalente à une attaque de déni de service, par laquelle une application légitime de consommateur de données peut n'être pas capable d'accéder à un certain contenu chez un fournisseur de contenu ou à sa version d'OPES.

Comme un flux OPES peut inclure des entités non OPES, il est susceptible d'attaques par interposition, par lesquelles un intrus peut injecter des instructions d'outrepassement dans le chemin des données. Ces attaques peuvent affecter la disponibilité des contenus ou perturber les techniques d'équilibrage de charge dans le réseau.

Les menaces ci-dessus surviennent aussi par des entités OPES compromises. Un intrus peut compromettre une entité OPES et ensuite utiliser des techniques d'interposition pour perturber la disponibilité des contenus chez une application de consommateur de données ou surcharger un serveur de fournisseur de contenu (essentiellement, une forme d'attaque de DoS).

Les attaquants peuvent utiliser l'instruction d'outrepassement pour affecter l'intégrité globale du système OPES. La capacité d'introduire des instructions d'outrepassement dans un flux de données peut affecter la comptabilité du système OPES. Elle peut aussi affecter la qualité du contenu qui est livré aux applications de consommateurs de données. Des menaces similaires peuvent survenir de mauvaises mises en œuvre de la facilité d'outrepassement.

Un outrepassement incohérent ou sélectif est aussi une menace. Ici, une extrémité peut essayer d'outrepasser un sous ensemble des entités OPES afin que le contenu résultant soit mal formé et subisse des défaillances ou compromette les entités qui traitent ce contenu (et s'attendent à ce que ce contenu soit complet et valide). De telles exceptions ne font souvent pas l'objet d'essais parce que les développeurs ne s'attendent pas à ce qu'un service vital disparaisse de la boucle de traitement.

D'autres menaces peuvent découler de la configuration des politiques de contrôle d'accès pour les entités OPES. Il est possible que des systèmes qui mettent en œuvre des contrôles d'accès via des entités OPES puissent être incorrectement configurés à honorer l'outrepassement, et donc, donnent un accès non autorisé à des intrus.

L'outrepassement de surveillance peut aussi être une menace. C'est parce que les systèmes qui mettent en œuvre la surveillance via des entités OPES peuvent être incorrectement configurés à honorer l'outrepassement, et donc, ignorer (laisser indétecté) du trafic avec des instructions d'outrepassement qui aurait dû être enregistré ou écouté. Il est aussi possible qu'une extrémité outrepasse des services comme l'examen de virus à l'extrémité receveuse. Cette menace peut être utilisée par des pirates pour injecter des virus à travers le réseau. Suivant la politique de l'IETF sur les écoutes [RFC2804], le modèle de communication OPES ne prend pas en compte les exigences pour les écoutes. Néanmoins, la menace documentée est réelle, non évidente, et les utilisateurs de la technologie OPES qui travaillent dans les écoutes ou des environnements d'enregistrement similaires devraient en être conscients.

D'autres questions de sécurité relatives au niveau application se trouvent dans la [RFC3837].

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)

[RFC3835] A. Barbir et autres, "Architecture pour les services marginaux à connexion libre (OPES)", août 2004. *(Information)*

[RFC3837] A. Barbir et autres, "Menaces et risques pour la sécurité des services marginaux à connexion libre (OPES)", août 2004. *(Information)*

[RFC3838] A. Barbir et autres, "Exigences de politique, d'autorisation, et de mise en application des services marginaux à connexion libre (OPES)", août 2004. *(Information)*

9.2 Références pour information

[RFC2804] IAB, IESG, "Politique de l'IETF en matière d'écoutes", mai 2000. *(Information)*

[RFC3238] S. Floyd, L. Daigle, "Considérations architecturales et de politique de l'IAB pour des services marginaux à connexion libre (OPES)", janvier 2002. *(Information)*

[RFC3752] A. Barbir et autres, "Services marginaux à connexion libre (OPES) : cas d'utilisation et scénarios de développement", avril 2004. *(Information)*

10. Remerciements

Plusieurs personnes ont contribué à ce travail. Tous nos remerciements à Alex Rousskov, Hilarie Orman, Oscar Batuner, Markus Huffman, Martin Stecher, Marshall Rose et Reinaldo Penno.

11. Adresse de l'auteur

Abbie Barbir
Nortel Networks
3500 Carling Avenue
Nepean, Ontario K2H 8E9
Canada

téléphone : +1 613 763 5229
mél : abbieb@nortelnetworks.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient 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 la Internet Society.