Groupe de travail Réseau
Request for Comments : 3837
Catégorie : Information

A. Barbir, Nortel Networks
O. Batuner, Independent consultant
B. Srinivas, Nokia
M. Hofmann, Lucent Technologies
H. Orman, Purple Streak Development

Traduction Claude Brière de L'Isle
août 2004

Menaces et risques pour la sécurité 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 norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright
Copyright (C) The Internet Society (2005).

Résumé
Le présent document examine les menaces pour la sécurité associées aux services marginaux à connexion libre (OPES, *Open Pluggable Edge Services*) et discute des effets des menaces pour la sécurité sur l'architecture sous-jacente. Le but principal de ce document est la découverte et l'analyse des menaces. Le document ne spécifie ni ne recommande aucune solution.

Table des matières

1. Introduction....1
2. Menaces pour les flux de données OPES....2
2.1 Menaces au niveau du réseau pour les flux OPES....3
2.2 Menaces au niveau de l'application pour le flux OPES....3
3. Menaces pour les données hors bande....5
3.1 Menaces qui mettent en danger le flux de données OPES....6
3. Informations de comptabilité inexactes....6
3.3 Répudiation de demande de service OPES....6
3.4 Politique de confidentialité incohérente....6
3.5 Exposition des préférences de confidentialité....6
3.6 Exposition des réglages de sécurité....6
3.7 Application impropre de la politique de confidentialité et de sécurité....6
3.8 Attaques de déni de service....7
4. Considérations sur la sécurité....7
5. Références....7
5.1 Références normatives....7
5.2 Références pour information....7
6. Remerciements....7
7. Adresse des auteurs....7
Déclaration complète de droits de reproduction....8

1. Introduction

L'architecture des services marginaux à connexion libre (OPES, *Open Pluggable Edge Services*) [RFC3835] permet des services d'application coopératifs (OPES services) 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 de données et le consommateur de données. Le processeur OPES peut répartir la responsabilité de l'exécution du service en communiquant et en collaborant avec un ou plusieurs serveurs d'invocation distants. Les détails de l'architecture OPES se trouvent dans la [RFC3835].

Les menaces pour la sécurité par rapport aux OPES peuvent être vues sous différents angles. Ce sont des risques pour la sécurité qui affectent le contenu des applications du consommateur, et celles qui affectent les applications de fournisseur de données. Ces menaces affectent la qualité et l'intégrité des données que les applications produisent ou consomment. D'un

autre côté, les risques pour la sécurité peuvent aussi être catégorisés en confiance à l'intérieur du système (c'est-à-dire, les fournisseurs de service OPES) et en protection du système contre les menaces imposées par des extérieurs comme des pirates et attaquants. Les infiltrés sont ces parties qui sont dans le système OPES. Les extérieurs sont les entités qui ne participent pas au système OPES.

On doit noter que tous sur le chemin de livraison OPES ne sont pas d'une confiance égale. Chaque domaine administratif de confiance OPES doit se protéger contre tous les extérieurs. De plus, il peut avoir une relation de confiance limitée avec un autre domaine administratif OPES pour certains objets.

Les fournisseurs de service OPES doivent utiliser l'authentification comme base de la construction de la confiance entre les domaines administratif. Des infiltrés peuvent intentionnellement ou involontairement infliger des torts et dommages aux applications de consommateur et de fournisseur de données. Ce peut être par une mauvaise configuration du système, par l'exécution d'un mauvais logiciel ou, si leurs réseaux sont compromis, par des pirates internes ou externes.

Selon le scénario de déploiement, la confiance au sein du système OPES se fonde sur un ensemble de relations transitives de confiance entre l'application de fournisseur de données, les entités OPES, et l'application de consommateur de données. Les menaces pour les entités OPES peuvent être au niveau du flux OPES et/ou au niveau du réseau.

En considérant les menaces pour le système OPES, le document suivra un modèle d'analyse des menaces qui identifie les menaces dans la perspective de comment elles vont affecter les applications de consommateur de données et de fournisseur de données.

Le but principal du document est la découverte et l'analyse des menaces. Le document ne spécifie ou recommande aucune solution.

Il est important de mentionner que l'architecture OPES a de nombreuses similarités avec d'autres réseaux dits en recouvrement, spécifiquement les antémémoires de la Toile et les réseaux de livraison de contenu (CDN, *content delivery network*) (voir les [RFC3752], [RFC3238]). Le présent document se concentre sur les menaces qui sont introduites par l'existence du processeur OPES et des serveurs d'invocation. Les menaces pour la sécurité spécifiques de services de contenu qui n'utilisent pas l'architecture OPES sont considérés comme sortant du domaine d'application de ce document. Cependant, ce document peut être utilisé comme entrée pour examiner les implications de sécurité des antémémoires de la Toile et des CDN.

Le document est organisé comme suit : la Section 2 discute des menaces pour les flux de données OPES sur le niveau réseau et application, la Section 3 discute des menaces aux autres parties du système, et la Section 4 discute des considérations de sécurité.

2. Menaces pour les flux de données OPES

Les menaces pour le flux de données OPES peuvent affecter les applications de consommateur de données et de fournisseur de données. Au niveau du flux OPES, des menaces peuvent se produire aux points d'application de politique et aux points de décision de politique [RFC3838], et le long du chemin du flux OPES lorsque des éléments de réseau sont utilisés pour traiter les données.

Un sérieux problème est posé par le simple fait que l'architecture OPES se fonde sur des protocoles largement adoptés (HTTP est utilisé comme exemple). Le document d'architecture exige spécifiquement que "la présence d'un processeur OPES dans le flux de demande/réponse de données NE DEVRA PAS interférer avec le fonctionnement de clients et serveurs sans capacité OPES". Cela facilite largement le déploiement des OPES, mais d'un autre côté, une grande majorité de clients (navigateurs) ne seront pas capables d'exploiter les sauvegardes ajoutées comme extensions au protocole de base.

Pour le consommateur de données normal, qui pourrait se poser des questions comme "d'où vient de contenu ? Puis-je l'avoir d'une autre façon ? Quelle est la différence ? Est-il légitime ?". Même si il y a des facilités et une expertise technique présentes pour creuser ces questions, un examen attentif de chaque résultat est d'un coût prohibitif en termes de temps et d'efforts. Les fournisseurs de contenu à capacité OPES peuvent essayer de se protéger en ajoutant des scripts de vérification et des structures de page spéciales. Les utilisateurs finaux à capacité OPES peuvent utiliser des outils spéciaux. Dans tous les autres cas (clients et serveurs sans capacité OPES) la protection va reposer sur des services de surveillance et l'investigation d'anomalies occasionnellement découvertes.

Un système OPES présente un danger particulier comme base possible pour des attaques par interposition classiques. Une des raisons pour lesquelles de telles attaques sont relativement rares est la difficulté de trouver une base appropriée : une combinaison de point d'interception de trafic contrôlant un large flux de données et une base de code d'application

fonctionnant sur un matériel à hautes performances avec des performances suffisantes pour analyser et éventuellement modifier toutes les données qui passent. Un processeur OPES répond à cette définition. Cela appelle à porter une attention particulière aux mesures de protection à tous les niveaux du système.

Toute compromission d'un processeur OPES ou d'un serveur d'invocation distant peut avoir un effet de "clapotement" sur les services OPES affectés à travers tous les fournisseurs de service qui utilisent le service. Pour atténuer cette menace, des procédures et outils de sécurité appropriés (par exemple, un pare-feu) devraient être appliqués.

Des menaces spécifiques peuvent exister au niveau du réseau et au niveau du flux de données OPES.

2.1 Menaces au niveau du réseau pour les flux OPES

Le processeur OPES et les serveurs d'invocation sont susceptibles d'attaques au niveau du réseau de la part d'extérieurs ou des réseaux d'autres fournisseurs de service OPES (c'est-à-dire, si le réseau d'un service OPES lié par contrat est compromis).

L'architecture OPES se fonde sur des protocoles d'application courants qui ne fournissent pas de fortes garanties de confidentialité, d'authentification, ou d'intégrité. Les considérations de l'IAB [RFC3238] exigent que l'adresse IP d'un processeur OPES soit accessible aux applications de consommateur de données au niveau de l'adressage IP. Cette exigence limite la capacité des fournisseurs de service à positionner le processeur OPES derrière des pare-feu et peut exposer le processeur OPES et les serveurs d'invocation distants à des attaques au niveau du réseau. Par exemple, l'utilisation de TCP/IP comme protocole de niveau réseau rend les processeurs OPES susceptibles de subir de nombreuses attaques connues, comme l'usurpation d'identité IP et le vol de session.

Le système OPES est aussi susceptible de subir un certain nombre de menaces pour la sécurité qui sont principalement associées à l'infrastructure du réseau. Ces menaces incluent l'espionnage, le déni de service, le sabotage, le vandalisme, l'espionnage industriel, et le vol de service.

Il y a des solutions de bonnes pratiques pour atténuer les menaces de niveau réseau. Il est recommandé que la sécurité des entités OPES au niveau réseau soit améliorée en utilisant les techniques et méthodes connues qui minimisent les risques d'usurpation d'identité IP, l'espionnage, le déni de service, et le vol de session.

Au niveau du flux OPES, la sécurité au niveau de la connexion entre le processeur OPES et les serveurs d'invocation est une considération importante. Par exemple, il est possible de tromper le processeur OPES ou le serveur d'invocation distant. Il y a des menaces sur la confidentialité des données entre le processeur OPES et le serveur d'invocation distant dans le flux OPES. Les paragraphes qui suivent couvrent les possibles attaques de déni de service sur un processeur OPES, un serveur d'invocation distant ou une application de consommateur de données, et la robustesse du réseau.

2.1.1 Déni de service pour les flux de connexion

Les processeurs OPES, les serveurs d'invocation, et les applications de consommateur de données peuvent être vulnérables aux attaques de déni de service. Elles peuvent être de divers types. Un exemple d'attaque de déni de service est la surcharge des processeurs OPES ou des serveurs d'invocation par des demandes parasites de service produites par un nœud malveillant, qui dénie au trafic de données légal les ressources nécessaires pour rendre le service. Les ressources incluent les cycles de CPU, la mémoire, les interfaces réseau, etc. Une attaque de déni de service peut être sélective, générique, ou aléatoire dans les termes selon lesquels les flux de communication sont affectés.

Une attaque de déni de service répartie est aussi possible quand un attaquant réussit à prendre la direction de plusieurs nœuds sur le réseau pour initier simultanément des demandes parasites de service à un processeur OPES (ou serveur d'invocation).

2.1.2 Menaces pour la robustesse du réseau

Si une mise en œuvre OPES viole les principes d'adressage de bout en bout, elle pourrait mettre en danger l'infrastructure de l'Internet en compliquant la gestion de l'acheminement et de la connexion. Si elle n'utilise pas les principes du contrôle de flux pour gérer les connexions, ou si elle interfère avec le contrôle de flux de bout en bout des connexions dont elle n'est pas à l'origine, cela pourrait causer l'encombrement de l'Internet.

Une mise en œuvre qui viole l'exigence de l'IAB d'un adressage explicite au niveau IP (par exemple, en ajoutant des capacités fonctionnelles d'OPES à un mandataire d'interception) peut réduire à néant certains mécanismes de protection et sauvegarde construits dans l'architecture OPES.

2.2 Menaces au niveau de l'application pour le flux OPES

Au niveau du contenu, les menaces pour le système OPES peuvent venir de l'extérieur ou de l'intérieur. La menace de l'extérieur est fréquemment intentionnelle. Les menaces de l'intérieur peuvent être intentionnelles ou accidentelles. Les accidents peuvent résulter d'erreurs de programmation ou de configuration qui résultent en un mauvais comportement du système.

Les problèmes et menaces de niveau application sur les systèmes OPES sont discutés ci-après :

2.2.1 Entités OPES non autorisées

Bien que l'autorisation de l'une des parties soit rendue obligatoire par l'architecture OPES, une telle autorisation se fait hors bande. La découverte de la présence d'une entité OPES et la vérification de l'autorisation exigent des actions spéciales et peuvent poser des problèmes.

L'ajout des informations de notification et d'autorisation aux messages de données (en utilisant des extensions au protocole de base) peut aider, en particulier si le logiciel du consommateur de données a connaissance de ces extensions.

2.2.2 Actions non autorisées d'entités OPES légitimes

Conformément à l'architecture OPES, l'autorisation n'est pas étroitement couplée à des règles et procédures spécifiques déclenchées par les règles. Même si était établie une exigence d'approbation de chaque règle et procédure particulière, il paraît au moins impraticable, sinon impossible, de demander une telle permission à l'utilisateur final. La granularité de l'autorisation s'étend aux classes de transformation, mais pas aux règles ou transformations individuelles. Les règles réelles et les procédures déclenchées peuvent (par malveillance ou à cause d'une erreur de programmation) effectuer des actions qui ne leur sont pas autorisées.

2.2.3 Transformations indésirables du contenu

Un service OPES autorisé peut effectuer des actions qui n'adhèrent pas aux attentes de la partie qui a donné l'autorisation du service. Les exemples peuvent inclure l'inondation d'annonces par un service local d'insertion d'annonces publicitaires ou l'utilisation d'une politique inappropriée par un service de filtrage de contenu.

D'un autre côté, une entité OPES agissant au nom d'une partie peut effectuer des transformations qu'une autre partie estime inappropriées. Des exemples peuvent inclure de remplacer les annonces initialement insérées par le fournisseur de contenu ou d'appliquer des transformations de filtrage qui changent la signification du texte.

2.2.4. Corruption du contenu

Le système OPES peut livrer des informations périmées ou par ailleurs déformées à cause de problèmes de programmation ou par suite d'attaques malveillantes. Par exemple, un serveur compromis, au lieu d'effectuer un service OPES, peut injecter un contenu bogué. Une telle action peut être un acte de cyber-vandalisme (incluant l'injection de virus) ou la distribution intentionnelle d'informations trompeuses (comme des manipulations de données financières).

Un serveur OPES compromis ou une entité malveillante dans le flux de données peut introduire des changements spécifiquement destinés à causer des actions impropres dans le serveur OPES ou le serveur d'invocation. Ces changements peuvent être dans le corps de message, dans les en-têtes, ou les deux. Ce type de menace est présenté plus en détails ci-dessous.

2.2.5 Menaces pour l'intégrité de structure du message

Un serveur OPES peut ajouter, retirer, ou supprimer certains en-têtes dans un message de demande et/ou réponse (par exemple, pour mettre en œuvre une protection de confidentialité supplémentaire ou aider au filtrage de contenu). De tels changements peuvent violer les exigences d'intégrité de bout en bout ou mettre en échec les services qui utilisent les informations fournies dans ces en-têtes (par exemple, des services de filtrage local ou des services fondés sur la référence).

2.2.6 Granularité de protection

Les services OPES ont la permission implicite de modifier le contenu. Cependant, les permissions ne s'appliquent généralement qu'à des portions du contenu, par exemple, les URL entre des étiquettes HTML particulières, du texte dans les titres, ou les URL correspondant à un schéma particulier. Pour exprimer de telles politiques, on doit être capable de se référer à des portions de messages et de détecter les modifications de parties du message.

Comme il y a actuellement très peu de soutien pour les politiques qui sont exprimées en termes de parties de message, il va être difficile d'attribuer une modification particulière à un processeur OPES particulier, ou de détecter automatiquement des violations de politique.

Un langage de politique à fine granularité devrait être conçu, et il pourrait être appliqué en utilisant des signatures numériques. Cela éviterait les problèmes inhérents aux mesures de protection de l'intégrité des données bond par bond (voir le paragraphe suivant).

2.2.7 Risques sur la protection bond par bond

Généralement, les services OPES ne peuvent pas être appliqués aux données protégées par des méthodes de chiffrement de bout en bout parce que la clé de déchiffrement ne peut pas être partagée avec les processeurs OPES sans compromettre la confidentialité des données à laquelle est destinée le chiffrement. Cela signifie que si la politique du point d'extrémité permet les services OPES, les données doivent soit être transmises sans protection de la confidentialité, soit qu'un autre modèle de chiffrement de bout en bout doit être développé, dans lequel la confidentialité est garantie bond par bond. Étendre le modèle de chiffrement de bout en bout sort du domaine d'application du présent travail.

Les services OPES qui modifient les données sont incompatibles avec les méthodes de protection de l'intégrité de bout en bout, et le présent travail ne tentera pas de définir de méthodes de protection de l'intégrité bond par bond.

2.2.8 Menaces pour l'intégrité de données complexes

Le système OPES peut violer l'intégrité des données en appliquant des transformations incohérentes à des objets de données en inter relations ou des références incohérentes au sein de l'objet de données. Les problèmes peuvent aller d'une structure de référence brisée (cibles modifiées/manquantes, références à de mauvaises localisations ou documents manquants) à un remplacement/suppression/insertion délibérée de liens qui violent les intentions du fournisseur du contenu.

2.2.9 Déni de service (DoS)

L'application du consommateur de données peut n'être pas capable d'accéder aux données si le système OPES a une défaillance pour une raison quelconque.

Un nœud malveillant ou fonctionnant mal peut être capable de bloquer tout le trafic. Le trafic de données destiné au processeur OPES (ou serveur d'invocation) peut n'être pas capable d'utiliser les services de l'appareil OPES. Le déni de service peut être réalisé en empêchant le trafic de données d'atteindre le processeur ou le serveur d'invocation.

2.2.10 Informations de traçage et de notification

Une mise en œuvre inadéquate ou vulnérable des mécanismes de traçage et de notification peut déjouer les sauvegardes construites dans l'architecture OPES.

Les facilités de traçage et de notification peuvent devenir une cible d'attaques malveillantes. De telles attaques peuvent créer des problèmes en découvrant et en arrêtant d'autres attaques.

L'absence d'une norme pour les informations de traçage et de notification peut poser un problème supplémentaire. Ces informations sont produites et consommées par des entités indépendantes (facilités de serveurs/agents d'utilisateur/fournisseur de contenu OPES). Il faudrait un ensemble de normes relatives à chaque protocole de base utilisé.

2.2.11 Communication non authentifiée dans un flux OPES

Il y a des risques et des menaces qui pourraient découler de communications non authentifiées entre le serveur OPES et les serveurs d'invocation. Manquer à utiliser une authentification forte entre processeurs OPES et serveurs d'invocation peut ouvrir des trous de sécurité par lesquels des attaques de DoS et d'autres types (voir les Sections 2 et 3) peuvent être effectuées.

3. Menaces pour les données hors bande

L'architecture OPES sépare un flux de données d'un flux d'informations de contrôle (chargement des jeux de règles, établissement de la confiance, traçage, propagation de la politique, etc.). Certaines exigences sont établies pour le premier, mais aucun mécanisme spécifique n'est prescrit. Cela donne plus de souplesse aux mises en œuvre, mais crée une charge supplémentaire aux développeurs et consommateurs potentiels pour s'assurer que chaque mise en œuvre spécifique satisfait à toutes les exigences pour la sécurité des données, l'authentification des entités, et l'autorisation des actions.

En plus d'effectuer des actions correctes sur le flux de données OPES, toute mise en œuvre OPES doit fournir un mécanisme adéquat pour satisfaire aux exigences pour les données hors bande et l'intégrité des informations de signalisation.

Quel que puisse être le mécanisme spécifique, il devient inévitablement l'objet de multiples menaces pour la sécurité et de possibles attaques. La façon dont les menaces et attaques peuvent être réalisées dépend des spécificités de la mise en œuvre mais les dommages résultants entrent généralement dans deux catégories : menaces pour le flux de données OPES et menaces pour l'intégrité des données.

Les menaces spécifiques sont :

3.1 Menaces qui mettent en danger le flux de données OPES

Toute faiblesse dans la mise en œuvre d'un mécanisme de sécurité, d'authentification, ou d'autorisation peut ouvrir la porte aux attaques décrites dans la Section 2.

Une mise en œuvre de système OPES devrait contrer toutes ces menaces et prouver sa robustesse et sa capacité à résister aux attaques malveillantes ou aux problèmes de réseautage et de programmation.

3. Informations de comptabilité inexactes

Collecter et faire rapport de données de comptabilité précises peut être vital quand des serveurs OPES sont utilisés pour étendre le modèle d'affaires d'un fournisseur de contenu, d'un fournisseur de service, ou comme base d'un service de tiers. La capacité à collecter et traiter de données de comptabilité est une partie importante de la fonction du système OPES. Cette fonctionnalité peut être mise au défi par la distorsion ou la destruction des données de comptabilité de base (généralement des enregistrements) des données comptables traitées, des paramètres de comptabilité, et de la configuration des rapports.

Par suite, un consommateur de données peut être facturé de façon inappropriée pour avoir vu des contenus qui n'ont pas réussi à être livrés, ou un fournisseur de contenu ou un fournisseur indépendant de services OPES peut n'être pas rétribué pour des services effectués.

Le système OPES peut utiliser les informations comptables pour répartir les ressources entre différents consommateurs ou limiter l'usage de ressources par un consommateur spécifique. Dans ce cas, une attaque sur le système comptable (par distorsion des données ou en produisant de fausses commandes de configuration) peut résulter en une gestion incorrecte des ressources et un déni de service par un blocage artificiel des ressources.

3.3 Répudiation de demande de service OPES

Une entité (producteur ou consommateur) peut faire une demande autorisée et plus tard prétendre qu'il n'a pas fait cette demande. Par suite, une entité OPES peut être tenue pour responsable de changements non autorisés au flux de données, ou sera incapable de recevoir la rétribution d'un service.

Une demande pour un service devrait être clairement formulée et il devrait y avoir une procédure claire pour agir au nom de toutes les parties. Cette action devrait avoir une demande, une action, un moyen non répudiable de vérifier la demande, et un moyen de spécifier l'effet de l'action.

3.4 Politique de confidentialité incohérente

Les entités OPES peuvent avoir des politiques de confidentialité qui ne sont pas cohérentes avec l'application du consommateur de données ou l'application du fournisseur de contenu.

Les problèmes relatifs à la confidentialité peuvent encore être compliqués si les entités OPES, les fournisseurs de contenu, et les utilisateurs finaux appartiennent à des juridictions différentes avec des exigences différentes et différents niveaux de protection légale. Par suite, l'utilisateur final peut n'être pas informé qu'il n'a pas la protection légale attendue. Le fournisseur de contenu peut être exposé à des risques judiciaires dus à un défaut de conformité à des réglementations dont il ignore tout.

3.5 Exposition des préférences de confidentialité

Le système OPES peut par inadvertance ou malveillance exposer les réglages et exigences de confidentialité de l'utilisateur final.

3.6 Exposition des réglages de sécurité

Il y a des risques que le système OPES puisse exposer les réglages de sécurité de l'utilisateur final quand il traite les demandes et réponses. Les données d'utilisateur doivent être traitées comme des informations de système sensibles et être protégées contre la divulgation accidentelle et délibérée.

3.7 Application impropre de la politique de confidentialité et de sécurité

Les entités OPES font partie du système de distribution de contenu et à ce titre ont une certaine obligation de prendre en charge les politiques de sécurité et confidentialité rendues obligatoires par le producteur de contenu et/ou l'utilisateur final. Cependant il y a un risque que ces politiques ne soient pas mises en œuvre et appliquées de façon appropriée.
L'application de consommateur de données peut ne pas savoir que ses protections ne sont plus effectives.

Il y a aussi la possibilité de fuites de sécurité et de confidentialité dues à une mauvaise configuration accidentelle ou, dues à l'incompréhension de quelles règles sont effectives pour un usager ou demande particulier.

Les parties des systèmes relatives à la confidentialité et la sécurité peuvent être prises pour cible par des attaques malveillantes et la capacité de resister à de telles attaques est d'une importance primordiale.

3.8 Attaques de déni de service

Les attaques de déni de service peuvent être de divers types. Une type d'attaque de DoS se fait en submergeant le client. Par exemple, un intrus peut amener un processeur OPES à produire de nombreuses réponses à un client. Il y a aussi un risque de DoS supplémentaire à partir d'une mauvaise configuration d'une règle qui ferait que le processeur OPES ignore une application de consommateur de données.

4. Considérations sur la sécurité

Le présent document discute des multiples questions de sécurité et de confidentialité relatives aux services OPES.

5. Références

5.1 Références normatives

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

[RFC3835] A. Barbir et autres, "Architecture pour les 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)*

5.2 Références pour 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)*

6. Remerciements

Un grand merci à T. Chan (Nokia) et A. Beck (Lucent).

7. Adresse des auteurs

Abbie Barbir
Nortel Networks
3500 Carling Avenue
Nepean, Ontario K2H 8E9
Canada
téléphone : +1 613 763 5229
mél : abbieb@nortelnetworks.com

Oskar Batuner
Independent consultant
mél : batuner@attbi.com

Bindignavile Srinivas
Nokia
5 Wayside Road
Burlington, MA 01803
USA
mél : bindignavile.srinivas@nokia.com

Markus Hofmann
Bell Labs/Lucent Technologies
Room 4F-513
101 Crawfords Corner Road
Holmdel, NJ 07733
US
mél : hofmann@bell-labs.com

Hilarie Orman
Purple Streak Development
téléphone : +1 732 332 5983
mél : ho@alum.mit.edu

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

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