Groupe de travail Réseau
Request for Comments : 4806
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Myers, TraceRoute Security LLC
H. Tschofenig, Siemens Networks GmbH
février 2007

Extensions du protocole d'état de certificat en ligne (OCSP) à IKEv2

Résumé
Bien que le protocole d'échange de clé Internet version 2 (IKEv2, *Internet Key Exchange Protocol version 2*) prenne en charge l'authentification fondée sur la clé publique, l'utilisation correspondante de listes de révocation de certificat (CRL, *Certificate Revocation List*) dans la bande est problématique à cause de la non limitation de taille de CRL. La taille d'une réponse du protocole d'état de certificat en ligne (OCSP, *Online Certificate Status Protocol*) est cependant bien encadrée et est petite. Le présent document définit l'extension "Contenu OCSP" à IKEv2. Une charge utile CERTREQ avec "Contenu OCSP" identifie zéro, un ou plusieurs répondants OCSP de confiance et est une demande d'inclusion d'une réponse OCSP dans la prise de contact IKEv2. Un receveur coopératif d'une telle demande répond avec une charge utile CERT contenant la réponse OCSP appropriée. Ce contenu est reconnaissable via le même identifiant "Contenu OCSP".

Quand des certificats sont utilisés avec IKEv2, les homologues communicants ont besoin d'un mécanisme pour déterminer l'état de révocation du certificat de l'homologue. OCSP est un de ces mécanismes. Le présent document s'applique quand OCSP est désiré et que la politique de sécurité empêche un des homologues IKEv2 d'accéder directement au répondant OCSP pertinent. Les pare-feu sont souvent déployés d'une manière qui empêche de tels accès par les homologues IKEv2 en dehors d'un réseau d'entreprise.

Table des matières

1. Introduction

La version 2 du protocole d'échangede clé Internet (IKE, *Internet Key Exchange*) [RFC4306] prend en charge une gamme de mécanismes d'authentification, incluant l'utilisation de l'authentification fondée sur la clé publique. La confirmation de la fiabilité du certificat est essentielle afin de réaliser les assurances de sécurité que fournit la cryptographie à clé publique.

Un élément fondamental d'une telle confirmation est la référence à l'état de révocation du certificat (voir dans la [RFC3280] des détails supplémentaires).

Le moyen traditionnel pour déterminer l'état de révocation de certificat est l'utilisation des listes de révocation de certificat (CRL, *Certificate Revocation List*). IKEv2 permet que les CRL soient échangées dans la bande via la charge utile CERT.

Cependant, les CRL peuvent croître sans limite de taille. De nombreux exemples existent dans la réalité pour montrer l'impraticabilité d'inclure un fichier de plusieurs mega octets dans un échange IKE. Cette contrainte est particulièrement aiguë dans les environnements limités en bande passante (par exemple, les communications avec des mobiles). L'effet net est l'exclusion des CRL dans la bande en faveur d'une acquisition hors bande (OOB, *out-of-band*) de ces données, si elles devraient même être utilisées.

S'appuyer sur des méthodes OOB peut être encore plus compliqué si l'accès aux données de révocation exige l'utilisation de IPsec (et donc d'IKE) pour établir un accès sûr et autorisé aux CRL d'un participant IKE. Une telle impasse de l'accès réseau contribue encore plus à réduire la confiance en l'état des révocations de certificat en faveur d'une confiance aveugle.

OCSP [RFC2560] offre une alternative utile. La taille d'une réponse OCSP est limitée et petite et donc convient pour la signalisation IKEv2 dans la bande de d'état de révocation d'un certificat.

Le présent document définit une extension à IKEv2 qui pemet l'utilisation de OCSP pour la signalisation dans la bande de l'état de révocation de certificat. Un nouveau codage de contenu est défini pour être utilisé dans les charges utiles CERTREQ et CERT. Une charge utile CERTREQ avec "Contenu OCSP" identifie zéro, un, ou plusieurs répondants OCSP de confiance et est une demande d'inclusion d'une réponse OCSP dans la prise de contact IKEv2. Un receveur coopératif à une telle demande répond par une charge utile CERT contenant la réponse OCSP appropriée. Ce contenu est reconnaissable via le même identifiant "Contenu OCSP".

2. 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].

Le présent document définit les termes suivants :

Demande OCSP : une demande OCSP se réfère à la charge utile CERTREQ qui contient un nouveau codage de contenu, appelé un contenu OCSP, qui se conforme à la définition et au comportement spécifiés au paragraphe 3.1.

réponse OCSP : une réponse OCSP se réfère à la charge utile CERT qui contient un nouveau codage de contenu, appelé un contenu OCSP, qui se conforme à la définition et au comportement spécifiés au paragraphe 3.2.

Répondant OCSP : le terme de répondant OCSP se réfère à l'entité qui accepte les demandes provenant d'un client OCSP et retourne des réponses comme défini dans la [RFC2560]. Noter que le répondant OCSP ne se réfère pas à la partie qui a envoyé le message CERT.

3. Définition de l'extension

En référence au paragraphe 3.6 de la [RFC4306], les valeurs pour le champ Codage de certificat de la charge utile CERT sont étendues comme suit (voir aussi la section Considérations relatives à l'IANA du présent document) :

Codage de certificat	**Valeur**
Contenu OCSP	14

3.1 Demande OCSP

Une valeur de Contenu OCSP (14) dans le champ Codage de certificat d'une charge utile CERTREQ indique la présence de zéro, un, ou plusieurs hachages de certificat de répondant OCSP dans le champ Autorité de certification de la charge utile CERTREQ. Le paragraphe 2.2 de la [RFC2560] définit les réponses, qui appartiennent à un des trois groupes suivants :

(a) la CA qui a produit le certificat,
(b) un répondant de confiance dont la clé publique est acceptée par le demandeur
(c) un répondant désigné par la CA (répondant autorisé) qui détient un certificat spécialement marqué produit directement par la CA, qui indique que le répondant peut produire des réponses OCSP pour cette CA.

Dans le cas (a), l'utilisation de hachages dans le message CERTREQ n'est pas nécessaire car la réponse OCSP est signée par la CA qui a produit le certificat. Dans le cas (c), la réponse OCSP est signée par le répondant désigné par la CA alors que l'envoyeur du message CERTREQ ne connaît pas la clé publique à l'avance. La présence du contenu OCSP dans un message CERTREQ va identifier un ou plusieurs répondants OCSP de confiance pour l'envoyeur dans le cas (b).

La présence du contenu OCSP (14) dans un message CERTREQ :
1. identifie zéro, un, ou plusieurs répondants OCSP de confiance pour l'envoyeur ;
2. notifie au receveur la prise en charge par l'envoyeur de l'extension OCSP à IKEv2; et
3. notifie au receveur le désir de l'envoyeur de recevoir la confirmation OCSP dans une charge utile CERT suivante.

3.2 Réponse OCSP

Une valeur de contenu OCSP (14) dans le champ Codage de certificat d'une charge utile CERT indique la présence d'une réponse OCSP dans le champ Données de certificat de la charge utile CERT.

La corrélation entre une charge utile CERT de réponse OCSP et une charge utile CERT correspondante portant un certificat peut être réalisée en confrontant le champ CertID de la réponse OCSP au certificat. Voir dans la [RFC2560] la définition du contenu de réponse OCSP.

4. Exigences d'extension

4.1 Demande de prise en charge de OCSP

Le paragraphe 3.7 de la [RFC4306] permet l'enchaînement de hachages d'ancres de confiance comme valeur de l'autorité de certification d'un seul message CERTREQ. Il n'y a cependant aucun moyen pour indiquer lequel parmi ces hachages, si il en est de présent, se rapporte au certificat d'un répondant OCSP de confiance.

Donc, une demande OCSP, comme définie au paragraphe 3.1 ci-dessus, est transmise séparément de toute autre charge utile CERTREQ dans un échange IKEv2.

Lorsque il est utile d'identifier plus d'un répondant OCSP de confiance, chacune de ces identifications DEVRA être enchaînée de manière identique à la méthode documentée au paragraphe 3.7 de la [RFC4306] concernant l'assemblage de multiples hachages d'ancres de confiance.

La valeur de l'autorité de certification dans une demande OCSP CERTREQ DEVRA être calculée et produite d'une manière identique à celle des hachages d'ancre de confiance documentée au paragraphe 3.7 de la [RFC4306].

À réception d'une charge utile CERT de réponse OCSP correspondant à une précédente demande OCSP CERTREQ, l'envoyeur CERTREQ DEVRA incorporer la réponse OCSP dans la logique de validation de chemin définie par la [RFC3280].

Noter que l'absence d'une charge utile CERT de réponse OCSP après l'envoi d'une charge utile CERT de demande OCSP pourrait être l'indication que cette extension OCSP n'est pas prise en charge. Par suite, il est recommandé que les nœuds soient configurés à n'exiger une réponse que si il est connu que tous les homoloques prennent bien en charge cette extension. Autrement, il est recommandé que les nœuds soient configurés à essayer OCSP et, si il n'y pas de réponse, de tenter de déterminer l'état de révocation de certificat par d'autres moyens.

4.2 Réponse à la prise en charge de OCSP

À réception d'une charge utile CERTREQ de demande OCSP, le receveur DEVRAIT acquérir l'assertion relative fondée sur OCSP et produire et transmettre une charge utile CERT de réponse OCSP correspondant au certificat nécessaire pour vérifier sa signature sur les charges utiles IKEv2.

Une charge utile CERT de réponse OCSP est transmise séparément de toute autre charge utile CERT dans un échange

IKEv2.

Les moyens par lesquels une réponse OCSP peut être acquise pour la production d'une charge utile CERT de réponse OCSP sort du domaine d'application du présent document.

Le champ Données de certificat d'une charge utile CERT de réponse OCSP DEVRA contenir une structure codée en DER OCSPResponse comme définie dans la [RFC2560].

5. Exemples et discussion

Cette section montre des exemples de messages IKEv2 standard avec les deux homologues, l'initiateur et le répondant, en utilisant l'authentification fondée sur la clé publique, les charges utiles CERTREQ et CERT. La première instance correspond au paragraphe 1.2 de la [RFC4306], dont les illustrations sont reproduites ci-dessous pour référence.

5.1 Homologue à homologue

L'application des extensions à IKEv2 définies dans le présent document pour l'échange d'homologue à homologue défini au paragraphe 1.2 de la [RFC4306] est comme suit. Les messages sont numérotés pour faciliter la référence.

Initiateur **Répondant**

(1) HDR, SAi1, KEi, Ni --------->

(2) <----- HDR, SAr1, KEr, Nr, CERTREQ(demande OCSP)

(3) HDR, SK {IDi, CERT(certificat),------>
CERT(réponse OCSP),
CERTREQ(demande OCSP),
[IDr,] AUTH, SAi2, TSi, TSr}

(4) <---- HDR, SK {IDr, CERT(certificat), CERT(réponse OCSP), AUTH, SAr2, TSi, TSr}

Extensions OCSP à l'IKEv2 de base

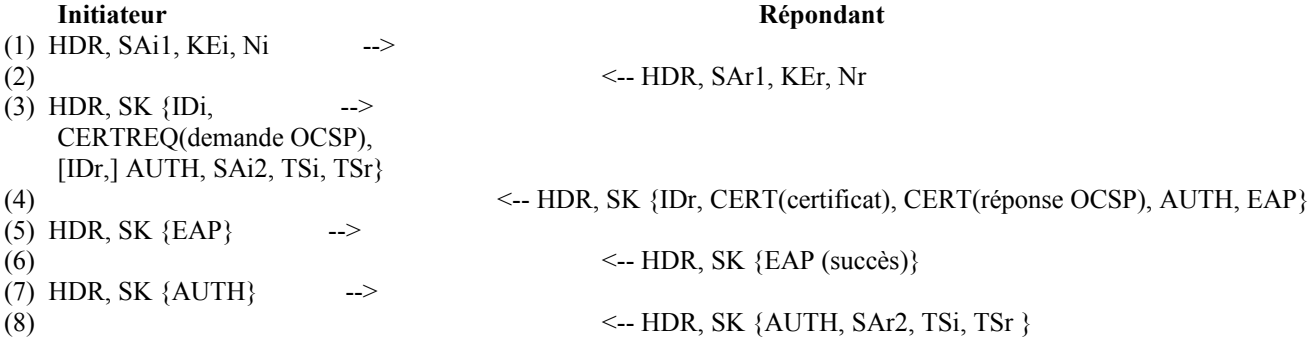
En (2), le répondant envoie une charge utile CERTREQ de demande OCSP identifiant zéro, un ou plusieurs répondants OCSP de confiance pour le répondant. En réponse, l'initiateur envoie en (3) à la fois une charge utile CERT portant son certificat et une charge utile CERT de réponse OCSP couvrant ce certificat. En (3), l'initiateur demande aussi une réponse OCSP via la charge utile CERTREQ de demande OCSP. En (4), le répondant retourne son certificat et une charge utile CERT de réponse OCSP séparée couvrant ce certificat.

Il est important de noter que dans ce scénario, le répondant dans (2) ne possède pas encore le certificat de l'initiateur et donc ne peut pas former une demande OCSP comme défini dans la [RFC2560]. Pour contourner ce problème, les hachages sont utilisés comme défini au paragraphe 4.1. Dans de telles instances, les demandes OCSP sont simplement des valeurs d'indice dans ces données. Donc, il est facilement déduit que les réponses OCSP peuvent être produites en l'absence d'une demande correspondante (pourvu que des noms occasionnels OCSP ne soient pas utilisés, voir la Section 6).

Il est aussi important qu'en étendant IKEv2 avec OCSP dans ce scénario, l'initiateur ait une connaissance certaine que le répondant est capable de participer à l'extension et veut le faire. Alors le répondant aura seulement à faire confiance à une ou plusieurs signatures de répondant OCSP. Ces facteurs motivent la définition de l'extension de hachage de répondant OCSP.

5.2 Protocole d'authentification étendu (EAP)

Un autre scénario très intéressant est l'utilisation de EAP pour s'accommoder de plusieurs utilisateurs finaux qui cherchent un accès d'entreprise à une passerelle IPsec. Noter que OCSP est utilisé pour la vérification de l'état du certificat du côté serveur du certificat IKEv2 et non pour les certificats qui peuvent être utilisés au sein des méthodes EAP (soit par l'homologue EAP, soit par le serveur EAP). Comme au paragraphe précédent, l'illustration qui suit est extraite de la [RFC4306]. En cas de conflit entre le présent document et la [RFC4306] concernant ces illustrations, c'est la [RFC4306] qui DEVRA l'emporter.



Extensions OCSP à EAP dans IKEv2

Dans le scénario EAP, les messages (5) à (8) ne sont pas pertinents pour le présent document.

6. Considérations sur la sécurité

Pour les raisons notées ci-dessus, une demande OCSP, comme définie au paragraphe 3.1, est utilisée à la place d'une syntaxe de demande OCSP pour déclencher la production et la transmission d'une réponse OCSP. OCSP, comme défini dans la [RFC2560], peut contenir une extension de demande de nom occasionnel pour améliorer la sécurité contre des attaques en répétition (voir les détails au paragraphe 4.4.1 de la [RFC2560]). La demande OCSP définie par le présent document ne peut pas s'accommoder de noms occasionnels. La [RFC2560] traite de cet aspect en pemettant des réponses pré produites.

La [RFC2560] s'attache à cette vulnérabilité à la répétition et indique : "L'utilisation de réponses précalculées permet des attaques en répétition dans lesquelles une vieille (bonne) réponse est répétée avant sa date d'expiration mais après que le certificat a été révoqué. Les déploiements de OCSP devraient évaluer avec soin les avantages des réponses pré calculées par rapport à la probabilité d'une attaque en répétition et les coûts associés à la réussite de son exécution". Les nœuds DEVRAIENT rendre configurable la fraîcheur requise d'une réponse OCSP.

7. Considérations relatives à l'IANA

Le présent document définit un nouveau type de champ à utiliser dans le champ Codage de certificat IKEv2 du format de charge utile Certificat. L'allocation officielle de l'extension "Contenu OCSP" du tableau de codage de certificat du paragraphe 3.6 de la [RFC4306] a été obtenue de l'IANA.

Codage de certificat	**Valeur**
OCSP Content	14

8. Remerciements

Les auteurs tiennent à remercier Russ Housley pour son soutien. De plus, nous souhaitons remercier Pasi Eronen, Nicolas Williams, Liqiang (Larry) Zhu, Lakshminath Dondeti, et Paul Hoffman de leur relecture. Pasi nous a donné un commentaire précieux lors du dernier appel. Merci aussi à Tom Taylor pour sa révision de Gen-ART. Jari Arkko nous a donné un commentaire de la relecture de l'IESG.

9. 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)

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin et C. Adams, "Protocole d'état de certificat en ligne d'infrastructure de clé publique X.509 pour l'Internet - OCSP", juin 1999. *(P.S.) (Remplacée par* RFC6960)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

Adresse des auteurs

Michael Myers
TraceRoute Security LLC
mél : mmyers@fastq.com

Hannes Tschofenig
Siemens Networks GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bavaria 81739 Germany
mél : Hannes.Tschofenig@siemens.com

Déclaration complète de droits de reproduction

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