

Groupe de travail Réseau
Request for Comments : 4483
 Catégorie : Sur la voie de la normalisation

E. Burger, Cantata Technology, Inc.
 mai 2006
 Traduction Claude Brière de L'Isle

Mécanismes pour le contenu indirect dans les messages du protocole d'initialisation de session (SIP)

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright

Copyright (C) The Internet Society (2006).

Résumé

Le présent document définit une extension à l'URL de type d'accès MIME "External-Body" pour satisfaire aux exigences de contenu indirect pour le protocole d'initialisation de session (SIP, *Session Initiation Protocol*). Ces extensions visent à permettre que toute partie MIME dans un message SIP soit référencée indirectement via un URI.

Table des matières

1. Introduction.....	2
2. Terminologie.....	2
3. Exemples de cas d'utilisation.....	2
3.1 Notification de présence.....	3
3.2 Partage de document.....	3
4. Exigences.....	4
5. Application de la RFC 2017 au problème du contenu indirect.....	4
5.1 Spécification de la prise en charge du contenu indirect.....	4
5.2 Prise en charge obligatoire des URI HTTP.....	4
5.3 Rejet du contenu indirect.....	4
5.4 Spécification de la localisation du contenu via un URI.....	5
5.5 Marquage de contenu indirect facultatif.....	5
5.6 Spécification des informations de version pour l'URI.....	5
5.7 Spécification de la durée de vie de l'URI.....	5
5.8 Spécification du type de contenu indirect.....	5
5.9 Spécification de la taille du contenu indirect.....	6
5.10 Spécification de l'objet du contenu indirect.....	6
5.11 Spécification de plusieurs URI pour le contenu indirect.....	6
5.12 Spécification d'une valeur de hachage pour le contenu indirect.....	7
5.13 Fourniture de commentaires supplémentaires sur le contenu indirect.....	7
5.14 Relations avec les en-têtes Call-Info, Error-Info, et Alert-Info.....	7
6. Exemples.....	7
6.1 Un seul contenu indirect.....	7
6.2 Multipart MIME avec contenu indirect.....	8
7. Considérations sur la sécurité.....	8
8. Contributions.....	9
9. Remerciements.....	10
10. Références.....	10
10.1 Références normatives.....	10
10.2 Références pour information.....	10
Adresse de l'auteur.....	10
Déclaration complète de droits de reproduction.....	11

1. Introduction

L'objet du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261] est de créer, modifier, ou terminer des sessions avec un ou plusieurs participants. Les messages SIP, comme les messages HTTP, sont syntaxiquement composés d'une ligne de début, d'un ou plusieurs en-têtes, et d'un corps facultatif. À la différence de HTTP, SIP n'est pas conçu comme un protocole de transport de données d'utilisation générale.

Il y a de nombreuses raisons qui font qu'il est souhaitable de spécifier indirectement le contenu du corps du message SIP. Pour les applications à bande passante limitée comme le cellulaire sans fil, l'adressage indirect donne le moyen d'annoter le contenu (indirect) avec des méta-données, qui peuvent être utilisées par le receveur pour déterminer de restituer ou non le contenu sur une liaison à ressources limitées.

Il est aussi possible que la taille du contenu à transférer submerge les mandataires de signalisation intermédiaires, accroissant inutilement ainsi la latence du réseau. Pour les applications SIP sensibles au temps, cela peut être inacceptable. Le contenu indirect peut remédier à cela en déplaçant le transfert de ce contenu hors du réseau de signalisation SIP et sur un canal de transfert de données potentiellement séparé.

Il peut aussi y avoir des scénarios où les données en rapport avec la session (le corps) qui ont besoin d'être transportées ne résident pas directement sur le point d'extrémité ou chez l'agent d'utilisateur. Dans de tels scénarios, il est souhaitable d'avoir un mécanisme par lequel le message SIP peut contenir une référence indirecte au contenu désiré. Le receveur va alors utiliser cette référence indirecte pour récupérer le contenu via un canal de transfert non SIP tel que HTTP, FTP, ou LDAP.

L'objet du contenu indirect est seulement de fournir un mécanisme de transport de remplacement pour les parties de corps MIME dans SIP. À l'exception du mécanisme de transport, les parties de corps indirectes sont équivalentes aux parties de corps en ligne, et devraient avoir le même traitement.

Les tentatives précédentes de solution du problème du contenu indirect utilisaient le type MIME `text/uri-list` [RFC2169]. Bien que séduisante par sa simplicité (une liste d'URI délimitée par des marqueurs de fin de ligne) elle n'a pas réussi à satisfaire un certain nombre d'exigences pour un mécanisme de contenu indirect dans SIP plus généraliste. Le manque le plus notable est la capacité à spécifier divers attributs sur la base de l'URI. Ces attributs peuvent inclure des informations de version, le type MIME du contenu référencé, etc.

La RFC 2017 définit un fort candidat pour le remplacement du type MIME `text/uri-list`. La [RFC2017] définit une extension au type MIME `message/external-body` défini à l'origine dans la [RFC2046]. L'extension que fait la RFC 2017 permet à un URI générique de spécifier la localisation du contenu plutôt que des paramètres spécifiques du protocole pour FTP, etc., comme le définit à l'origine la RFC2046. Bien qu'elle fournisse la plupart des fonctionnalités nécessaires pour un mécanisme de contenu indirect SIP, la RFC 2017 par elle-même n'est pas une solution complète. Le présent document spécifie l'usage de la RFC 2017 nécessaire pour satisfaire aux exigences mentionnées pour le contenu indirect.

Les exigences peuvent être classées comme s'appliquant à l'URI, qui fait référence indirectement au contenu désiré, ou comme s'appliquant au contenu lui-même. Lorsque possible, les paramètres MIME et en-têtes d'entité existants sont utilisés pour satisfaire ces exigences. Les paramètres MIME (`Content-Type`) sont la manière préférée pour décrire l'URI, tandis que les en-têtes d'entité sont la manière préférée de décrire le contenu (indirect). Voir dans la [RFC2045] la description de la plupart de ces en-têtes d'entité et paramètres MIME.

2. Terminologie

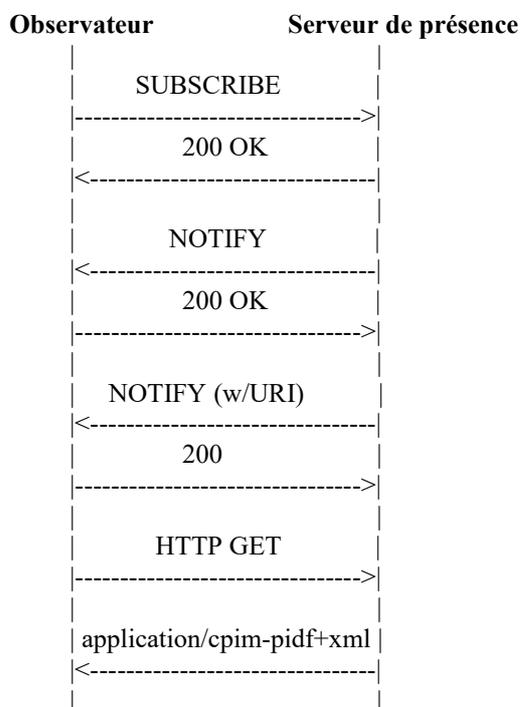
Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Exemples de cas d'utilisation

Il y a plusieurs exemples d'utilisation du mécanisme de contenu indirect. Ce sont seulement des exemples et ils ne sont pas destinés à limiter la portée ou l'applicabilité du mécanisme.

3.1 Notification de présence

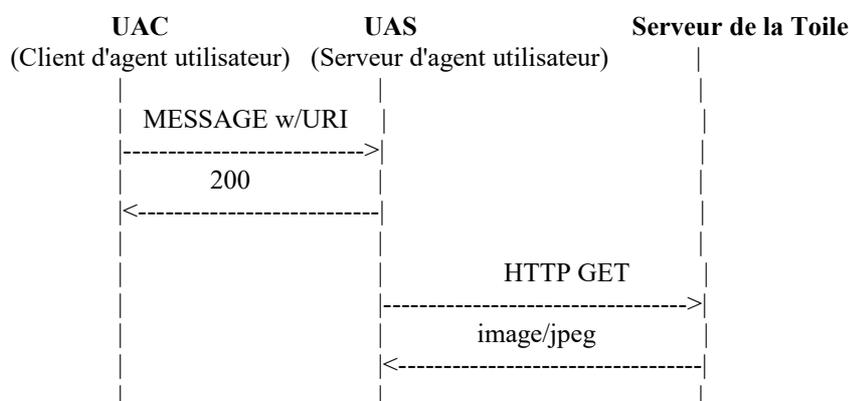
Les informations portées dans un document de présence pourraient excéder la taille recommandée pour une demande SIP (NOTIFY) en particulier si le document porte des informations agrégées provenant de plusieurs points d'extrémité. Dans une telle situation, il va être souhaitable d'envoyer la demande NOTIFY avec un pointeur indirect sur le document de présence, qui va alors être restitué, par exemple, par HTTP.



Dans cet exemple, le serveur de présence retourne un URI HTTP pointant sur un document de présence sur le serveur de présence, que l'observateur peut alors aller chercher en utilisant un HTTP GET.

3.2 Partage de document

Durant une conversation de messagerie instantanée, un service utile est le partage de document, par lequel une partie envoie un IM (demande de MESSAGE) avec un pointeur indirect sur un document qui est destiné à être rendu par la partie distante. Porter un tel document directement dans la demande MESSAGE n'est pas une utilisation appropriée du canal de signalisation. De plus, le document à partager peut résider sur un serveur complètement indépendant de celui de la partie génératrice.



Dans cet exemple, un UAC utilisateur souhaite échanger une image JPEG qu'il a mémorisée sur son serveur de la Toile avec l'UAS d'utilisateur avec lequel il a une conversation IM. Il a l'intention de rendre le JPEG en ligne dans la conversation IM. Le receveur de la demande MESSAGE lance une demande HTTP GET au serveur de la Toile pour récupérer l'image JPEG.

4. Exigences

- o Il DOIT être possible de spécifier la localisation du contenu via un URI. De tels URI DOIVENT se conformer à la [RFC3986].
- o Il DOIT être possible de spécifier la longueur du contenu indirect.
- o Il DOIT être possible de spécifier le type du contenu indirect.
- o Il DOIT être possible de spécifier la disposition de chaque URI de façon indépendante.
- o Il DOIT être possible d'étiqueter chaque URI pour identifier si et quand le contenu référencé par cet URI a changé. Les applications de ce mécanisme peuvent envoyer le même URI plus d'une fois. L'intention de cette exigence est de permettre au receveur de déterminer si le contenu référencé par cet URI a changé, sans avoir à récupérer ce contenu. Des exemples de la façon dont l'URI pourrait être étiqueté incluent un numéro de séquence, un horodatage, et un numéro de version. Quand il est utilisé avec HTTP, le mécanisme d'étiquette d'entité (ETAG) défini dans la [RFC2616], peut être approprié. Noter qu'on étiquette pas l'URI lui-même mais le contenu auquel l'URI se réfère, et que l'étiquette est donc effectivement une "métadonnée" du contenu même.
- o Il DOIT être possible de spécifier la durée pendant laquelle un certain URI est valide. Ce peut ou non être la même que la durée de vie du contenu lui-même.
- o Il DOIT être possible pour l'UAC et l'UAS d'indiquer la prise en charge de ce mécanisme de contenu indirect. Un mécanisme de repli DEVRAIT être spécifié pour le cas où une des parties est dans l'incapacité de prendre en charge le contenu indirect.
- o Il DOIT être possible à l'UAC et l'UAS de négocier le type du contenu indirect lors de l'utilisation du mécanisme de contenu indirect.
- o Il DOIT être possible à l'UAC et l'UAS de négocier la prise en charge de tout schéma d'URI à utiliser dans le mécanisme de contenu indirect. Ceci est en plus de la capacité de négocier le type de contenu.
- o Il DEVRAIT être possible d'assurer l'intégrité et la confidentialité de l'URI quand il est reçu par la partie distante.
- o Il DOIT être possible de traiter le contenu indirect sans intervention humaine.
- o Le transfert indirect du contenu DOIT être permis dans tout message SIP qui porterait autrement ce contenu comme corps.

5. Application de la RFC 2017 au problème du contenu indirect

Le texte qui suit décrit l'application de la RFC 2017 aux exigences de contenu indirect.

5.1 Spécification de la prise en charge du contenu indirect

Un UAC/UAS indique la prise en charge du contenu indirect en incluant le type MIME message/external-body dans l'en-tête Accept. L'UAC/UAS PEUT fournir des valeurs supplémentaires dans l'en-tête Accept pour indiquer les types de contenu qu'il veut accepter, soit directement, soit par contenu indirect. Les agents d'utilisateur qui prennent en charge le contenu indirect DOIVENT prendre en charge le contenu indirect de type application/sdp MIME.

Par exemple : Accept: message/external-body, image/*, application/sdp

5.2 Prise en charge obligatoire des URI HTTP

Les applications qui utilisent ce mécanisme de contenu indirect DOIVENT prendre en charge le schéma d'URI HTTP. Des schémas d'URI supplémentaires PEUVENT être utilisés, mais un UAC/UAS DOIT prendre en charge la réception d'un URI HTTP pour un contenu indirect si il annonce la prise en charge du contenu indirect.

L'UAS PEUT annoncer d'autres schémas d'accès dans le paramètre "schemes" de l'en-tête Contact dans la réponse de l'UAS à la demande d'établissement de session de l'UAC (par exemple, INVITE, SUBSCRIBE) comme décrit dans la [RFC3840].

5.3 Rejet du contenu indirect

Si un UAS reçoit une demande SIP qui contient une charge utile de contenu indirect et si l'UAS ne peut pas ou ne veut pas prendre en charge un tel type de contenu, il DOIT rejeter la demande avec une réponse 415 Type de support non pris en charge, comme défini au paragraphe 21.4.13 de SIP [RFC3261]. En particulier, l'UAC devrait noter l'absence du type message/external-body MIME dans l'en-tête Accept de cette réponse pour indiquer que l'UAS ne prend pas en charge le

contenu indirect, ou l'absence du type MIME particulier du commentaire demandé pour indiquer que l'UAS ne prend pas en charge ce type de support particulier.

5.4 Spécification de la localisation du contenu via un URI

L'URI pour le contenu indirect est spécifié dans un paramètre "URI" du type MIME message/external-body. Un paramètre access-type indique que le contenu externe est référencé par un URI. Les spécifications d'URI HTTP DOIVENT se conformer à la [RFC3986].

Par exemple :

```
Content-Type: message/external-body; access-type="URL";
URL="http://www.exemple.com/the-indirect-content"
```

5.5 Marquage de contenu indirect facultatif

Certains contenus ne sont pas critiques pour le contexte de la communication si il y a un échec de récupération ou de conversion. Le mécanisme de contenu indirect utilise le mécanisme Critical-Content décrit dans la [RFC3459]. En particulier, si l'UAS est incapable d'aller chercher ou de rendre une partie de corps facultative, le serveur NE DOIT PAS retourner une erreur à l'UAC.

5.6 Spécification des informations de version pour l'URI

Afin de déterminer si le contenu indirectement référencé par l'URI a changé, un en-tête d'entité Content-ID est utilisé. La syntaxe de cet en-tête est définie dans la [RFC2045]. Les changements au contenu sous-jacent référencé par un URI DOIVENT résulter en un changement du Content-ID associé à cet URI. Plusieurs messages SIP portant des URI qui se réfèrent au même contenu DEVRAIENT réutiliser le même Content-ID, pour permettre au receveur de mettre ce contenu en antémémoire et éviter des récupérations inutiles. Le Content-ID est destiné à être unique au monde et DEVRAIT être temporairement unique sur les dialogues SIP.

Par exemple : Content-ID: <4232423424@www.exemple.com>

5.7 Spécification de la durée de vie de l'URI

L'URI fourni par l'en-tête Content-Type n'est pas nécessairement accessible ou valide pendant un temps infini. Le fournisseur de l'URI DOIT plutôt spécifier la période pendant laquelle cet URI est valide et accessible. Ceci est fait par le paramètre "EXPIRATION" de Content-Type. Le format de ce paramètre d'expiration est une valeur "date-time" de la [RFC1123]. Il est de plus restreint par la présente application à utiliser seulement l'heure GMT, en cohérence avec l'en-tête Date: de SIP. C'est un paramètre obligatoire. Noter que la gamme des valeurs de date-time peut aller de minutes à des jours ou même des années. Par exemple :

```
Content-Type: message/external-body;
expiration="Mon, 24 June 2002 09:00:00 GMT"
```

5.8 Spécification du type de contenu indirect

Pour prendre en charge les mécanismes SIP existants pour la négociation des types de contenu, un en-tête d'entité Content-Type DEVRAIT être présent dans l'entité (la charge utile) elle-même. Si le protocole (schéma) de l'URI prend en charge ses propres mécanismes de négociation de contenu (par exemple, HTTP) cet en-tête peut être omis. L'expéditeur DOIT, cependant, être prêt à ce que le receveur rejette le contenu indirect si il est incapable de négocier un type MIME approprié en utilisant le protocole sous-jacent pour le schéma d'URI.

Par exemple :

```
Content-Type: message/external-body; access-type="URL";
expiration="Mon, 24 June 2002 09:00:00 GMT";
URL="http://www.exemple.com/the-indirect-content"
<CRLF>
```

```
Content-Type: application/sdp
Content-Disposition: session
<CRLF>
```

5.9 Spécification de la taille du contenu indirect

Quand elle est connue à l'avance, la taille du contenu indirect en octets DEVRAIT être fournie via un paramètre de taille sur l'en-tête Content-Type. C'est une extension de la RFC 2017 mais est en ligne avec les autres types d'accès définis pour le type MIME message/external-body dans la RFC 2046. La taille du contenu est utile pour le receveur afin de déterminer si il va récupérer le contenu. Comme avec le contenu fourni directement, un UAS peut retourner une réponse d'erreur 513 dans le cas où la taille de contenu est trop grande. La taille (size) est un parameter facultatif.

Par exemple :

```
Content-Type: message/external-body; access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.com/the-indirect-content";
  size=4123
```

5.10 Spécification de l'objet du contenu indirect

Un en-tête d'entité Content-Disposition DOIT être présent pour tout contenu indirect.

Par exemple :

```
Content-Type: message/external-body; access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.com/the-indirect-content"
<CRLF>
Content-Type: image/jpeg
Content-Disposition: render
```

5.11 Spécification de plusieurs URI pour le contenu indirect

Si il est besoin d'envoyer plusieurs URI pour un contenu indirect, un type MIME multiparties [RFC2046] approprié devrait être utilisé. Chaque URI DOIT être contenu dans une seule entité. Le contenu indirect peut être mêlé à du contenu fourni directement. Ceci est particulièrement utile avec le type MIME multipart/alternative.

Note : la présente spécification ne change pas la signification des diverses variantes de multipart, en particulier multipart/related, comme décrit dans la [RFC2387].

Par exemple :

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=boundary42

--boundary42
Content-Type: text/plain; charset=us-ascii

L'annonce de la compagnie pour juin 2002 suit :
--boundary42
Content-Type: message/external-body;
  access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.com/announcements/07242002";
  size=4123
Content-Type: text/html
Content-Disposition: render
--boundary42--
```

5.12 Spécification d'une valeur de hachage pour le contenu indirect

Si l'expéditeur connaît le contenu spécifique référencé par la référence indirecte, et si il souhaite que le receveur soit capable de valider que ce contenu n'a pas été altéré par rapport à celui prévu par l'expéditeur, il va inclure un hachage SHA-1 [RFC3174] du contenu. Si il est inclus, le hachage est codé en étendant la syntaxe MIME [RFC2046] pour inclure un paramètre "hash" pour le type de contenu "message/ external-body", dont la valeur est un codage hexadécimal du hachage.

Par exemple :

```
Content-Type: message/external-body;
  access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.com/the-indirect-content.au";
  size=52723;
  hash=10AB568E91245681AC1B
<CRLF>
Content-Disposition: render
```

5.13 Fourniture de commentaires supplémentaires sur le contenu indirect

On PEUT utiliser l'en-tête d'entité Content-Description pour fournir un texte facultatif de forme libre pour commenter le contenu indirect. Ce texte PEUT être affiché à l'utilisateur final mais NE DOIT PAS être utilisé par les autres éléments pour déterminer la disposition du corps.

Par exemple :

```
Content-Type: message/external-body;
  access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.com/the-indirect-content";
  size=52723
<CRLF>
Content-Description: Multicast gaming session
Content-Disposition: render
```

5.14 Relations avec les en-têtes Call-Info, Error-Info, et Alert-Info

SIP [RFC3261] définit trois en-têtes qui fournissent des informations supplémentaires à l'égard d'une session, d'une réponse d'erreur particulière, ou d'une alerte. Ces trois en-têtes permettent à l'UAC ou l'UAS d'indiquer des informations supplémentaires au moyen d'un URI. Ils peuvent être considérés comme une forme de contenu indirect. Le mécanisme de contenu indirect défini dans le présent document n'est pas destiné à remplacer ces en-têtes. Les en-têtes définis dans SIP DOIVENT plutôt être utilisés de préférence au présent mécanisme, lorsque applicable, à cause de la sémantique bien définie de ces en-têtes.

6. Exemples

6.1 Un seul contenu indirect

```
INVITE sip:boromir@exemple.com SIP/2.0
From: <sip:gandalf@exemple.net>;tag=347242
To: <sip:boromir@exemple.com>
Call-ID: 3573853342923422@exemple.net
CSeq: 2131 INVITE
Accept: message/external-body application/sdp
Content-Type: message/external-body;
  ACCESS-TYPE=URL;
  URL="http://www.exemple.net/party/06/2002/announcement";
```

```

EXPIRATION="Sat, 20 Jun 2002 12:00:00 GMT";
size=231
Content-Length: 105
Content-Type: application/sdp
Content-Disposition: session
Content-ID: <4e5562cd1214427d@exemple.net>

```

6.2 Multipart MIME avec contenu indirect

```

MESSAGE sip:boromir@exemple.com SIP/2.0
From: <sip:gandalf@exemple.net>;tag=34589882
To: <sip:boromir@exemple.com>
Call-ID: 9242892442211117@exemple.net
CSeq: 388 MESSAGE
Accept: message/external-body, text/html, text/plain, image/*, text/x-emoicon
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=zz993453

```

```

--zz993453
Content-Type: message/external-body;
  access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.net/company_picnic/image1.png";
  size=234422

```

```

Content-Type: image/png
Content-ID: <9535035333@exemple.net>
Content-Disposition: render
Content-Description: Kevin fait trempette dans la pataugeoire

```

```
--zz993453
```

```

Content-Type: message/external-body;
  access-type="URL";
  expiration="Mon, 24 June 2002 09:00:00 GMT";
  URL="http://www.exemple.net/company_picnic/image2.png";
  size=233811

```

```

Content-Type: image/png
Content-ID: <1134299224244@exemple.net>
Content-Disposition: render
Content-Description: Pierre sur son tricycle

```

```
--zz993453--
```

7. Considérations sur la sécurité

Tout mécanisme de contenu indirect introduit des problèmes de sécurité supplémentaires. Par nature, le contenu indirect exige une étape de traitement et de transfert d'informations supplémentaire. Il y a un certain nombre d'abus potentiels du mécanisme de contenu indirect:

- o Le contenu indirect permet à l'initiateur de choisir un autre protocole avec une sécurité plus faible ou des vulnérabilités connues pour le transfert de contenu (par exemple, demandant au receveur de produire une demande HTTP qui résulte en un défi d'authentification de base).
- o Le contenu indirect permet à l'initiateur de demander au receveur de consommer des ressources supplémentaires dans le transfert d'informations et le traitement du contenu, créant potentiellement une voie pour des attaques de déni de service (par exemple, un URL FTP actif consommant deux connexions pour chaque message de contenu indirect).

- o Le contenu indirect pourrait être utilisé comme une forme d'attaque d'examen d'accès où l'URL de contenu indirect est en fait un URL fallacieux pointant sur une ressource interne du receveur. La réponse à la demande de contenu indirect pourrait révéler des informations sur les accès ouverts (et vulnérables) sur ces ressources internes.
- o Un URL de contenu indirect peut divulguer des informations sensibles sur l'initiateur comme un nom d'utilisateur interne (au titre d'un URL HTTP) ou éventuellement des informations de géolocalisation.

Heureusement, toutes ces menaces potentielles peuvent être atténuées par un examen attentif à la fois des URL de contenu indirect reçus et de ceux qui sont envoyés. La protection de l'intégrité et de la confidentialité de l'URI de contenu indirect peut empêcher aussi des attaques.

Pour la confidentialité, l'intégrité, et l'authentification, ce mécanisme de contenu indirect s'appuie sur les mécanismes de sécurité mentionnés dans la RFC 3261. En particulier, l'usage de S/MIME comme défini à la Section 23 de la RFC 3261 fournit les mécanismes nécessaires pour assurer l'intégrité, la protection, et la confidentialité de l'URI de contenu indirect et des paramètres associés.

Sécuriser le transfert du contenu indirect est de la responsabilité du protocole sous-jacent utilisé pour ce transfert. Si HTTP est utilisé, les applications qui mettent en œuvre cette méthode de contenu indirect DEVRAIENT prendre en charge le schéma d'URI HTTPS pour un transfert sûr du contenu et DOIVENT prendre en charge la mise à niveau des connexions avec TLS, en utilisant starttls. Noter qu'un échec de réalisation de HTTPS ou de starttls (par exemple, à cause d'une discordance de certificat ou de chiffrement) après avoir accepté le contenu indirect dans la demande SIP n'est pas la même chose que de rejeter la demande SIP, et cela peut exiger des communications d'utilisateur à utilisateur supplémentaires pour sa correction.

Noter que le présent document ne plaide pas en faveur de l'utilisation d'une confiance transitive. C'est à dire que juste parce que l'UAS reçoit un URI d'un UAC auquel l'UAS se fie, l'UAS NE DEVRAIT PAS faire implicitement confiance à l'objet référencé par l'URI sans établir sa propre relation de confiance avec le fournisseur de l'URI.

Le contrôle d'accès au contenu référencé par l'URI n'est pas défini par la présente spécification. Des mécanismes de contrôle d'accès peuvent être définis par le protocole pour le schéma de l'URI de contenu indirect.

Si l'UAC connaît le contenu à l'avance, il DEVRAIT inclure un paramètre de hachage dans le contenu indirect. Le paramètre de hachage est un hachage SHA-1 codé en hexadécimal [RFC3174] du contenu indirect. Si une valeur de hachage est incluse, le receveur DOIT vérifier le contenu indirect par rapport à ce hachage et indiquer toute discordance à l'utilisateur.

De plus, si le paramètre de hachage est inclus et si l'URI cible implique d'établir un contexte de sécurité utilisant des certificats, l'UAS DOIT ignorer le résultat de la procédure de validation de certificat, et vérifier à la place que le hachage du contenu (canonisé) reçu correspond au hachage présenté dans le paramètre de hachage du contenu indirect.

Si le paramètre de hachage n'est PAS inclus, l'expéditeur DEVRAIT utiliser seulement des schémas qui offrent l'intégrité de message (comme https:). Quand le paramètre de hachage n'est pas inclus et que la sécurité utilisant des certificats est utilisée, l'UAS DOIT vérifier tous les certificats de serveur, en utilisant la liste de l'UAS des autorités de certificat de confiance de niveau supérieur.

Si le hachage du contenu indirect n'est pas utilisé, le contenu retourné au receveur par l'exercice de la référence indirecte peut avoir été altéré par rapport à celui prévu par l'expéditeur.

8. Contributions

Sean Olson, seanol@microsoft.com, a fourni la grande majorité du contenu du présent document, incluant la fonction d'éditeur jusqu'à la première revue par l'IESG review. Dean Willis l'a retouché ensuite.

Eric Burger a édité le document et traité les commentaires de l'IESG, incluant le mécanisme de négociation du protocole d'accès.

9. Remerciements

Cullen Jennings et Nancy Greene ont effectué une relecture attentive et fourni des commentaires et suggestions précieux.

10. Références

10.1 Références normatives

- [RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – [Application et prise en charge](#)", STD 3, octobre 1989. (*MàJ par RFC7766*)
- [RFC2017] N. Freed, K. Moore, A. Cargille, "Définition du [type d'accès de corps extérieur](#) MIME d'URL", octobre 1996. (*P.S.*)
- [RFC2045] N. Freed et N. Borenstein, "[Extensions de messagerie Internet](#) multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. (*D. S., MàJ par 2184, 2231, 5335.*)
- [RFC2046] N. Freed et N. Borenstein, "[Extensions de messagerie Internet](#) multi-objets (MIME) Partie 2 : Types de support", novembre 1996. (*D. S., MàJ par 2646, 3798, 5147, 6657, 8098*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (*MàJ par RFC8174*)
- [RFC2169] R. Daniel, "Convention triviale pour l'[utilisation de HTTP dans la résolution d'URN](#)", juin 1997. (*Expérimentale*)
- [RFC2616] R. Fielding et autres, "[Protocole de transfert hypertexte](#) -- HTTP/1.1", juin 1999. (*D.S., MàJ par 2817, 6585*)
- [RFC3174] D. Eastlake 3 et P. Jones, "[Algorithme US de hachage](#) sécurisé n° 1 (SHA1)", sept. 2001. (*Info, MàJ par 4634 et 6234*)
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002. (*Mise à jour par 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760*)
- [RFC3459] E. Burger, "[Paramètres à contenu critique](#) des extensions multi-usage de messagerie Internet (MIME)", janvier 2003. (*P.S.*)
- [RFC3840] J. Rosenberg, H. Schulzrinne et P. Kyzivat, "[Indication des capacités d'agent d'utilisateur](#) dans le protocole d'initialisation de session (SIP)", août 2004
- [RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "[Identifiant de ressource uniforme](#) (URI) : Syntaxe générique", STD 66, janvier 2005. (*P.S. ; MàJ par RFC8820*)

10.2 Références pour information

- [RFC2387] E. Levinson, "Type de [contenu MIME Multiparti/Relatif](#)", août 1998. (*P.S.*)

Adresse de l'auteur

Eric Burger (editor)
Cantata Technology, Inc.

mél : eburger@cantata.com
URI : <http://www.cantata.com>

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2006).

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 fournis 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 encloses ne viole 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 pourrait 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 fourni par l'activité de soutien administratif (IASA) de l'IETF.