Groupe de travail Réseau
Request For Comments : 1847
Catégorie : En cours de normalisation

J. Galvin
S. Murphy
Trusted Information Systems
S. Crocker, CyberCash, Inc.
N. Freed, Innosoft International, Inc.

Traduction Claude Brière de L'Isle
octobre 1995

Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée

Résumé
Le présent document définit un cadre au sein duquel des services de sécurité peuvent être appliqués à des parties de corps MIME. Les extensions de messagerie Internet multi objets (MIME, *Multipurpose Internet Mail Extensions*) définissent le format des contenus des messages électroniques de l'Internet et traitent des corps des messages multi-parties textuels et non textuels. Les nouveaux types de contenu sont des sous-types de "multipart:" signé et chiffré. Chacun contiendra deux parties de corps : une pour les données protégées, et une pour les informations de contrôle nécessaires pour retirer la protection. Le type et le contenu des parties de corps des informations de contrôle sont déterminés par la valeur du paramètre de protocole du type de contenu multipart/signé ou multipart/chiffré qui les contient, dont il est exigé qu'il soit présent.

Table des matières

1. Introduction

Un message électronique Internet comporte deux parties : l'en-tête et le corps. Les en-têtes forment une collection de paires de champ/valeur structurées conformément au STD 11, [RFC0822], tandis que le corps, si il est structuré, est défini conformément à MIME [RFC1521]. La spécification MIME de base n'apporte aucune protection spécifique pour la sécurité.

Le présent document définit un cadre dans lequel la protection de la sécurité fournie par d'autres protocole peut être utilisée avec MIME de façon complémentaire. Par lui-même, il ne spécifie aucune protection de sécurité. Un agent MIME doit inclure la prise en charge à la fois du cadre défini ici et du mécanisme pour interagir avec un protocole de sécurité défini dans un autre document. Le service combiné résultant fournit la sécurité pour les messages en une seule partie et multiparties textuels et non textuels.

Le cadre est fournit en définissant deux nouveaux sous-types de sécurité du type de contenu multiparties MIME : signé et chiffré. Dans chacun des sous types de sécurité, il y a exactement deux parties de corps qui sont concernées : une pour les données protégées et une pour les informations de contrôle. Le type et le contenu de la partie de corps d'informations de contrôle sont déterminés par la valeur du paramètre de protocole du type de contenu multipart/signed ou multipart/encrypted englobant, qui est obligatoirement présent. En enregistrant de nouvelles valeurs pour le paramètre protocole exigé, le cadre est facilement extensible pour s'accommoder de divers protocoles.

Un agent MIME qui prend en charge ce cadre sera capable de reconnaître une partie de corps multiparties de sécurité et d'identifier ses données protégées et ses parties de corps d'informations de contrôle. Si la valeur du paramètre de protocole n'est pas reconnue, l'agent MIME ne sera pas capable de traiter la multipartie de sécurité. Cependant, un agent MIME peut continuer à traiter toutes les autres parties de corps qui seraient présentes.

2. Définition des sous-types de sécurité pour les multiparties

Le type de contenu multipart/signed spécifie comment prendre en charge les services d'authentification et d'intégrité via la signature numérique. Les informations de contrôle sont portées dans la seconde des deux parties de corps exigées.

Le type de contenu multipart/encrypted spécifie comment prendre en charge la confidentialité via le chiffrement. Les informations de contrôle sont portées dans la première des deux parties de corps exigées.

Un processus en trois étapes est décrit pour la génération et la réception des contenus multipart/signed et multipart/encrypted. Les détails du traitement effectué durant chaque étape sont spécifiés par le protocole de sécurité utilisé.

2.1 Définition de Multipart/Signed

(1) Nom de type MIME : multipart
(2) Nom de sous-type MIME : signed
(3) Paramètres exigés : boundary, protocol, et micalg
(4) Paramètres facultatifs : aucun
(5) Considérations pour la sécurité :Doit être traité comme opaque pendant le transit.

Le type de contenu multipart/signed contient exactement deux parties de corps. La première partie de corps est celle sur laquelle la signature numérique a été créée, incluant ses en-têtes MIME. La seconde partie de corps contient les informations de contrôle nécessaires pour vérifier la signature numérique. La première partie de corps peut contenir tout type de contenu MIME valide, étiqueté en conséquence. La seconde parti de corps est étiquetée conformément à la valeur du paramètre de protocole.

Le jeton d'attribut pour le paramètre de protocole est "protocol", c'est-à-dire,

paramètre := "protocole" "=" valeur

Le jeton valeur comporte les jetons type et sous-type de l'en-tête Content-Type: de la seconde partie de corps, c'est-à-dire,

valeur := <"> type "/" sous-type <">

où les jetons de type et sous-type sont définis par la spécification MIME [RFC1521]. La sémantique du paramètre protocole est définie conformément à sa valeur.

Le jeton d'attribut pour le paramètre micalg est "micalg", c'est-à-dire,

paramètre := "micalg" "=" valeur

Vérification d'intégrité de message (MIC, *Message Integrity Check*) est le nom donnée à la quantité calculée sur la partie de corps avec un résumé de message ou une fonction de hachage, pour la prise en charge du service de signature numérique. Les jetons de valeur valides sont définis par la spécification qui donne la valeur du paramètre de protocole. La valeur peut être une liste de jetons séparés par une virgule (","), indiquant l'utilisation de plusieurs algorithmes de MIC. Il en résulte que le caractère virgule (",") est explicitement exclu de la liste des caractères qui peuvent être inclus dans un jeton utilisé comme valeur du paramètre micalg. Si plusieurs algorithmes de MIC sont spécifiés, l'objet et l'usage des divers algorithmes sont définis par le protocole. Si l'algorithme de MIC est aussi spécifié dans les informations de contrôle et si la valeur qui y est n'est pas en accord avec la valeur dans ce paramètre, ce doit être traité comme une erreur.

Note : La présence du paramètre micalg dans l'en-tête de type de contenu multipart/signed est explicitement destinée à prendre en charge un traitement en un seul passage. Les mises en œuvre de MIME peuvent localiser la seconde partie de corps en entrant la première partie de corps et en calculant les valeurs de MIC spécifiées jusqu'à ce que la limite identifiant la seconde partie de corps soit trouvée.

Le contenu entier du conteneur de la multipart/signed doit être traité comme opaque pendant qu'il est en transit entre son générateur et son receveur. Les agents de transfert de message intermédiaires ne doivent altérer d'aucune façon le contenu d'une multipart/signed, y compris, mais sans s'y limiter, de changer le codage du transfert de contenu de la partie de corps ou d'aucune de ses parties de corps encapsulées.

La signature dans une multipart/signed ne s'applique qu'au matériel qui est réellement au sein de l'objet multipart/signed. En particulier, elle ne s'applique à aucun des matériaux qui enveloppent le message, pas plus qu'elle ne s'applique aux entités qui y sont référencées (par exemple via un corps externe de message MIME) plutôt que incluses dans le contenu signé.

Lors de la création d'une partie de corps multipart/signed, la séquence d'étapes suivante décrit le traitement nécessaire. On doit souligner que ces étapes sont descriptives, et ne sont pas des prescriptions, et qu'elles n'imposent en aucune façon de restrictions ou d'exigences aux mises en œuvre de la présente spécification.

(1) Le contenu de la partie de corps à protéger est préparé selon une convention locale. Le contenu est alors transformé en une partie de corps MIME en format MIME canonique, incluant un jeu approprié d'en-têtes MIME.

De plus, si l'objet multipart/signed devait être transféré sur l'infrastructure SMTP Internet standard, le corps MIME résultant serait restreint au 7 bits – c'est à dire que l'utilisation de matériaux exigeant un codage de transfert de contenu à 8 bits ou binaire n'est pas admis. De tels matériaux à 8 bits ou binaires NE DOIVENT PAS être codés en utilisant le codage quoted-printable ou base64.

La raison d'être de cette exigence est qu'il n'est généralement pas possible, étant données les caractéristiques actuelles du SMTP de l'Internet, qu'un générateur de message garantisse qu'un message ne va voyager que sur des chemins capables de porter du matériel à 8 bits ou binaire.

Les clients SMTP ont normalement l'option de convertir le message pour éliminer l'utilisation de codages en 8 bits ou binaire ou de retourner à l'origine une notification de non livraison. Cependant, la conversion n'est pas viable dans le cas des objets signés car la conversion invaliderait nécessairement la signature. Cela laisse comme seule option disponible la notification de non livraison, ce qui n'est pas acceptable.

(2) La partie de corps (en-têtes et contenu) à signer numériquement est préparée pour la signature conformément à la valeur du paramètre de protocole. Les en-têtes MIME de la partie de corps signée sont inclus dans la signature pour protéger l'intégrité de l'étiquetage MIME des données qui sont signées.

(3) La partie de corps préparée est mise à disposition du processus de création de signature conformément à une convention locale. Le processus de création de signature doit mettre à la disposition d'une mise en œuvre MIME deux flux de données : les informations de contrôle nécessaires pour vérifier la signature, que les mises en œuvre MIME vont placer dans la seconde partie de corps et étiqueter conformément à la valeur du paramètre protocole, et la partie de corps signée numériquement, que la mise ne œuvre MIME utilisera comme première partie de corps.

En recevant une partie de corps multipart/signed, la séquence d'étapes suivante décrit le traitement nécessaire pour vérifier la ou les signatures. On doit souligner que ces étapes ne sont que descriptives, et ne constituent pas des prescriptions, et qu'elles n'imposent en aucun cas des restrictions ou des exigences aux mises en œuvre de la présente spécification.
(1) La première partie de corps et les informations de contrôle dans la seconde partie de corps doivent être prêtes pour le processus de vérification de signatures conformément à la valeur du paramètre protocole.

(2) Les parties de corps préparées doivent être mises à la disposition du processus de vérification de signature conformément à une convention locale. Le processus de vérification de signature doit mettre à la disposition des mises en œuvre de MIME le résultat de la vérification de signature et la partie de corps qui a été signée numériquement.

Note : Le résultat de la vérification de signature va vraisemblablement inclure une sorte de "testament" de la réussite ou de l'échec de la vérification. Aussi, dans le cas normal, la partie de corps retournée après vérification de signature sera la même que la partie de corps qui avait été reçue. On n'insiste pas sur le fait que ceci est le cas pour permettre les protocoles qui pourraient modifier la partie de corps durant le traitement de la signature.

(3) Le résultat du processus de vérification de signature est mis à la disposition de l'usager et la mise en œuvre MIME continue le traitement avec la partie de corps vérifiée, c'est à dire, la partie de corps retournée par le processus de vérification de signature.

L'exemple qui suit est une illustration d'une partie de corps multipart/signed. Elles est nécessairement incomplète car les informations de contrôle sont définies par le protocole de sécurité, qui doit être spécifié dans un autre document.

Content-Type: multipart/signed; protocol="TYPE/STYPE"; micalg="MICALG"; boundary="Signed Boundary"

--Signed Boundary
Content-Type: text/plain; charset="us-ascii"

Ici se trouverait le texte à signer qui pourrait être de n'importe quel type de données, étiqueté bien sûr en conséquence.

--Signed Boundary
Content-Type: TYPE/STYPE

Ici se trouveraient les informations de contrôle pour le "TYPE/STYPE" de protocole

--Signed Boundary--

2.2 Définition de Multipart/Encrypted

(1) Nom de type MIME : multipart
(2) Nom de sous-type MIME : encrypted
(3) Paramètres exigés : boundary, protocol
(4) Paramètres facultatifs : aucun
(5) Considérations pour la sécurité : aucune

Le type de contenu multipart/encrypted contient exactement deux parties de corps. La première partie de corps contient les informations de contrôle nécessaires pour déchiffrer les données de la seconde partie de corps et sont étiquetées conformément à la valeur du paramètre de protocole. La seconde partie de corps contient les données qui ont été chiffrées et qui est toujours étiquetée application/octet-stream.

Le jeton d'attribut pour le paramètre de protocole est "protocol", c'est à dire,

paramètre := "protocole" "=" valeur

Le jeton de valeur comporte les jetons de type et de sous-type de l'en-tête Content-Type: de la première partie de corps, c'est à dire,

valeur := <"> type "/" sous-type <">

où les jetons de type et de sous-type sont définis par la spécification MIME [RFC1521]. La sémantique du paramètre protocole est définie conformément à sa valeur.

Lors de la création d'une partie de corps multipart/encrypted, la séquence d'étapes suivante décrit le traitement nécessaire. On doit souligner que ces étapes sont purement descriptives, et ne sont pas des prescriptions, et qu'elles n'imposent en aucune façon de restrictions ou d'exigences aux mises en œuvre de la présente spécification.

(1) Le contenu de la partie de corps à protéger est préparé selon une convention locale. Le contenu est alors transformé en partie de corps MIME en format canonique MIME, incluant un jeu approprié d'en-têtes MIME.

(2) La partie de corps (en-têtes et contenu) à chiffrer est préparée pour le chiffrement conformément à la valeur du paramètre protocole. Les en-têtes MIME de la partie de corps chiffrée sont inclus dans le chiffrement pour protéger contre la divulgation l'étiquetage MIME des données qui sont chiffrées.

(3) La partie de corps préparée est mise à la disposition du processus de chiffrement conformément à une convention locale. Le processus de chiffrement doit mettre à la disposition d'une mise en œuvre MIME deux flux de données : les informations de contrôle nécessaires pour déchiffrer la partie de corps, que la mise en œuvre MIME va placer dans la première partie de corps et étiqueter conformément à la valeur du paramètre protocole, et la partie de corps chiffrée, que la mise en œuvre MIME va placer dans la seconde partie de corps et étiqueter application/octet-stream. Donc, lorsque elles sont utilisées dans une multipart/encrypted, les données application/octet-stream comportent une partie de corps MIME incorporée.

Lors de la réception d'une partie de corps multipart/encrypted, la séquence d'étapes suivante décrit le processus nécessaire pour déchiffrer les données incluses. On doit souligner que ces étapes ne sont que descriptives, et ne sont pas des prescriptions, et qu'elles n'imposent en aucune façon de restrictions ou d'exigences aux mises en œuvre de la présente

spécification.

(1) La seconde partie de corps et les informations de contrôle de la première partie de corps doivent être préparées pour le processus de déchiffrement conformément à la valeur du paramètre de protocole.

(2) La partie de corps préparée doit être mise à la disposition du processus de déchiffrement conformément à une convention locale. Le processus de déchiffrement doit mettre à la disposition de la mise en œuvre MIME le résultat du déchiffrement et la forme déchiffrée de la partie de corps chiffrée.

Note : Le résultat du processus de déchiffrement va vraisemblablement inclure un "testament" sur le succès ou l'échec du déchiffrement. L'échec peut être dû à l'incapacité de localiser la bonne clé de déchiffrement ou le bon champ de receveur, etc. Les mises en œuvre devraient noter que les données, si il en est, d'un processus de déchiffrement qui a échoué sont à peu près sûres de passer à la poubelle.

(3) Le résultat du processus de déchiffrement est mis à la disposition de l'usager et la mise en œuvre MIME continue le traitement de la partie de corps déchiffrée, c'est-à-dire, la partie de corps retournée par le processus de déchiffrement.

Note : Une mise en œuvre MIME ne sera pas capable d'afficher la forme reçue de la seconde partie de corps parce que l'application de chiffrement va transformer la partie de corps. Cette transformation ne sera pas décrite dans les en-têtes MIME (Content-Type: et Content-Transfer-Encoding:) mais elle sera plutôt décrite dans le contenu de la première partie de corps. Donc, une mise en œuvre devrait attendre que le chiffrement ait été retiré avant de tenter d'afficher le contenu.

L'exemple suivant est une illustration d'une partie de corps multipart/encrypted. Il est nécessairement incomplet car les informations de contrôle sont définies par le protocole de sécurité, qui doit être spécifié dans un autre document.

Content-Type: multipart/encrypted; protocol="TYPE/STYPE"; boundary="Encrypted Boundary"

--Encrypted Boundary
Content-Type: TYPE/STYPE

Les informations de contrôle pour le "TYPE/STYPE" de protocole se trouveraient ici

--Encrypted Boundary
Content-Type: application/octet-stream

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

Tout ce texte en retrait, y compris les en-têtes , seraient illisible car il aurait été chiffré par le "TYPE/STYPE" du protocole. Aussi, ces données chiffrées pourraient être de n'importe quel type de données, étiquetées en conséquence, bien sûr.

--Encrypted Boundary--

3. Définition des types de contenu d'informations de contrôle

Le présent document définit un cadre au sein duquel les services de sécurité peuvent être appliqués aux parties de corps MIME. Une mise en œuvre MIME minimale sera capable de reconnaître les parties de corps multipart/signed et multipart/encrypted et sera capable d'identifier en leur sein les parties de corps de données protégées et d'informations de contrôle.

La prise en charge complète des services de sécurité exige que l'agent MIME reconnaisse la valeur du paramètre de protocole et continue le traitement sur la base de sa valeur. La valeur du paramètre de protocole est la même que celle utilisée pour étiqueter le type de contenu des informations de contrôle.

La valeur du paramètre de protocole et le traitement exigé résultant doivent être spécifiés dans le document qui définit le protocole de sécurité utilisé. Ce document doit aussi spécifier précisément le contenu de la partie de corps d'informations de contrôle.

4. Définition des types de contenu de gestion de clés

La présente spécification reconnaît que la spécification complète d'un protocole de sécurité fondés sur MIME doit comporter un mécanisme pour distribuer le matériel cryptographique utilisé à l'appui des services de sécurité. Par exemple, un service de signature numérique mis en œuvre avec une cryptographie asymétrique exige qu'une clé publique du signataire soit disponible pour celui qui la vérifie.

Un mécanisme possible pour la distribution du matériel cryptographique est de définir deux parties de corps supplémentaires : une pour les besoins de la demande des informations cryptographiques et une pour retourner les informations cryptographiques demandées. La spécification d'un protocole de sécurité peut comporter une définition de deux parties de corps de ce genre ou elle peut spécifier un autre mécanisme pour la distribution du matériel cryptographique.

5. Considérations pour la sécurité

La présente spécification décrit une amélioration à MIME pour prendre en charge les parties de corps signées et chiffrées. Dans ce contexte, la totalité du document est consacrée à la sécurité.

6. Remerciements

David H. Crocker a suggéré l'utilisation d'une structure multiparties pou l'interaction MIME - PEM .

7. Références

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC5322*)

[RFC1521] N. Borenstien et N. Freed, "MIME (Extensions multi-usage de messagerie Internet) Partie 1 : Mécanismes pour spécifier et décrire le format des corps de message Internet", septembre 1993. *(Rendue obsolète par les RFC 2045 à 2049)*

8. Adresse des auteurs

Jim Galvin
Trusted Information Systems
3060 Washington Road
Glenwood, MD 21738
téléphone : +1 301 854 6889
fax : +1 301 854 5363
mél : galvin@tis.com

Sandy Murphy
Trusted Information Systems
3060 Washington Road
Glenwood, MD 21738
téléphone : +1 301 854 6889
fax: +1 301 854 5363
mél : sandy@tis.com

Steve Crocker
CyberCash, Inc.
2086 Hunters Crest Way
Vienna, VA 22181
téléphone : +1 703 620 1222
fax : +1 703 391 2651
mél : crocker@cybercash.com

Ned Freed
Innosoft International, Inc.
1050 East Garvey Avenue South
West Covina, CA 91790
téléphone : +1 818 919 3600
fax : +1 818 919 3614
mél : ned@innosoft.com