Groupe de travail Réseau
Request for Comments : 3207
RFC rendue obsolète : 2487
Catégorie : En cours de normalisation

P. Hoffman, Internet Mail Consortium
février 2002

Traduction Claude Brière de L'Isle

Extension de service à SMTP pour SMTP sûr sur la sécurité de couche transport

Résumé
Le présent document décrit une extension au service de protocole simple de transfert de messagerie 'SMTP, *Simple Mail Transfer Protocol*) qui permet au serveur et au client SMTP d'utiliser la sécurité de couche transport (TLS, *Transport Layer Security*) pour assurer des communications confidentielles et authentifiées sur l'Internet. Cela donne aux agents SMTP la capacité de protéger certaines de leurs communications, ou toutes, contre l'espionnage et les agressions.

1. Introduction

Les serveurs et clients SMTP [RFC2821] communiquent normalement en clair sur l'Internet. Dans de nombreux cas, cette communication passe par un ou plusieurs routeurs qui ne sont ni contrôlés ni de confiance par et pour aucune des deux entités. Un tel routeur qui n'est pas de confiance pourrait permettre à un tiers de surveiller ou altérer les communications entre le serveur et le client.

De plus, il est souvent désiré que deux agents SMTP soient capables d'authentifier les identités de l'un et de l'autre. Par exemple, un serveur SMTP sûr pourrait ne permettre les communications qu'avec les agents SMTP qu'il connaît, ou il pourrait agir différemment pour les messages reçus d'un agent qu'il connaît et ceux d'un agent qu'il ne connaît pas.

TLS [RFC2246], plus couramment connu sous le nom de SSL, est un mécanisme populaire pour améliorer les communications TCP avec la confidentialité et l'authentification. TLS est largement utilisé avec le protocole HTTP, et est aussi utilisé pour ajouter de la sécurité à de nombreux autres protocoles courants qui fonctionnent sur TCP.

Le présent document rend obsolète la RFC 2487.

1.1 Terminologie

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Extension STARTTLS

L'extension STARTTLS à SMTP se présente comme suit :
(1) le nom du service SMTP défini ici est STARTTLS ;
(2) la valeur de mot clé EHLO associée à l'extension est STARTTLS ;
(3) le mot clé STARTTLS n'a aucun paramètre ;
(4) un nouveau verbe SMTP, "STARTTLS", est défini ;
(5) aucun paramètre supplémentaire n'est ajouté à aucune commande SMTP.

3. Mot clé STARTTLS

Le mot clé STARTTLS est utilisé pour dire au client SMTP que le serveur SMTP est actuellement capable de négocier l'utilisation de TLS. Il ne prend pas de paramètre.

4. Commande STARTTLS

Le format de la commande STARTTLS est :

STARTTLS

sans paramètre.

Après que le client a donné la commande STARTTLS, le serveur répond par un des codes de réponse suivants :

220 Prêt à commencer TLS
501 Erreur de syntaxe (pas de paramètre permis)
454 TLS indisponible pour des raisons temporaires

Si le client reçoit la réponse 454, il doit décider si il continue ou non la session SMTP. Une telle décision se fonde sur la politique locale. Par exemple, si TLS était utilisé pour l'authentification du client,celui-ci pourrait essayer de continuer la session, au cas où le serveur le permettrait même sans authentification. Cependant, si TLS a été négocié pour le chiffrement, un client qui reçoit une réponse 454 a besoin de décider si il envoie de toutes façons le message sans chiffrement TLS, si il attend pour réessayer plus tard, ou si il abandonne et notifie l'erreur à l'envoyeur.

Un serveur TLS publiquement référencé NE DOIT PAS exiger l'utilisation de l'extension STARTTLS pour livrer un message en local. Cette règle empêche l'extension STARTTLS de porter atteinte à l'interopérabilité de l'infrastructure SMTP de l'Internet. Un serveur SMTP publiquement référencé est un serveur SMTP qui fonctionne sur l'accès 25 d'un hôte Internet figurant sur la liste des enregistrements MX (ou des enregistrements A si un enregistrement MX n'est pas présent) pour le nom de domaine du côté droit d'une adresse de messagerie Internet.
Tout serveur SMTP peut refuser d'accepter des messages en relais sur la base d'une authentification fournie durant la négociation TLS. Un serveur SMTP qui n'est pas publiquement référencé peut refuser d'accepter des messages en relais ou en livraison locale sur la base de l'authentification fournie durant la négociation TLS.

Un serveur SMTP qui n'est pas publiquement référencé peut choisir de demander que le client effectue une négociation TLS avant d'accepter toute commande. Dans ce cas, le serveur DEVRAIT retourner le code de réponse :

530 Doit produire d'abord une commande STARTTLS

à toute commande autre que NOOP, EHLO, STARTTLS, ou QUIT. Si le client et le serveur utilisent l'extension ENHANCEDSTATUSCODES ESMTP [RFC2034], le code d'état à retourner DEVRAIT être 5.7.0.

Après réception d'une réponse 220 à une commande STARTTLS, le client DOIT commencer la négociation TLS avant de donner toute autre commande SMTP. Si, après avoir produit la commande STARTTLS, le client découvre que certaines défaillances l'empêchent en fait de commencer une prise de contact TLS, il DEVRAIT alors interrompre la connexion.

Si le client SMTP utilise l'intubation telle que définie dans la RFC2920, la commande STARTTLS doit être la dernière commande dans un groupe.

4.1 Traitement après la commande STARTTLS

Après l'achèvement de la prise de contact TLS, les deux parties DOIVENT immédiatement décider si elles continuent ou non sur la base de l'authentification et la confidentialité réalisées. Le client et le serveur SMTP peuvent décider de continuer même si la négociation TLS s'est terminée sans authentification et/ou sans confidentialité parce que la plupart des services SMTP sont effectués sans authentification ni confidentialité, mais certains clients ou serveurs SMTP peuvent vouloir ne continuer que si un niveau particulier d'authentification et/ou de confidentialité a été obtenu.

Si le client SMTP décide que le niveau d'authentification ou de confidentialité n'est pas assez élevé pour qu'il continue, il DEVRAIT produire une commande SMTP QUIT immédiatement après l'achèvement de la négociation TLS. Si le serveur

SMTP décide que le niveau d'authentification ou de confidentialité n'est pas assez élevé pour qu'il continue, il DEVRAIT répondre à chaque commande SMTP provenant du client (autre qu'une commande QUIT) avec le code de réponse 554 (avec une éventuelle chaîne de texte telle que "Commande refusée à cause du manque de sécurité").

La décision de croire ou non à l'authenticité de l'autre partie dans une négociation TLS est une affaire locale. Cependant, les règles générales pour la décision sont que :
- un client SMTP va probablement ne vouloir authentifier qu'un serveur SMTP dont le certificat de serveur a un nom de domaine qui est le nom de domaine auquel le client pense qu'il se connecte ;.
- un serveur SMTP publiquement référencé va probablement vouloir accepter tout certificat vérifiable provenant d'un client SMTP, et va éventuellement vouloir mettre des informations distinctives sur le certificat dans l'en-tête Received des messages qui ont été relayés ou soumis par le client.

4.2 Résultat de la commande STARTTLS

À l'achèvement de la prise de contact TLS, le protocole SMTP est remis à l'état initial (l'état de SMTP après qu'un serveur a produit un message de bienvenue 220 service prêt). Le serveur DOIT éliminer toutes les informations obtenues du client, comme l'argument de la commande EHLO, qui n'ont pas été obtenues de la négociation TLS elle-même. Le client DOIT éliminer toutes les informations obtenues du serveur, comme la liste des extensions de service SMTP, qui n'ont pas été obtenues de la négociation TLS elle-même. Le client DEVRAIT envoyer une commande EHLO comme première commande après une négociation TLS réussie.

La liste des extensions de service SMTP retournée en réponse à une commande EHLO reçue après la prise de contact TLS PEUT être différente de la liste retournée avant la prise de contact TLS. Par exemple, un serveur SMTP pourrait ne pas vouloir annoncer la prise en charge d'un mécanisme SASL particulier [RFC2222] sauf si le client a envoyé un certificat de client approprié durant la prise de contact TLS.

Le client et le serveur DOIVENT savoir tous deux si il y a une session TLS active. Un client NE DOIT PAS tenter de commencer une session TLS si il y en a déjà une active. Un serveur NE DOIT PAS retourner l'extension STARTTLS en réponse à une commande EHLO reçue après l'achèvement d'une prise de contact TLS.

4.3 STARTTLS sur l'accès de soumission

STARTTLS est une extension ESMTP valide lorsque utilisée sur l'accès de soumission, comme défini dans la [RFC2476]. En fait, comme l'accès de soumission n'est pas, par définition, un serveur SMTP publiquement référencé, l'extension STARTTLS peut être particulièrement utile en fournissant la sécurité et l'authentification pour ce service.

5. Exemple d'utilisation

Le dialogue suivant illustre comment un client et un serveur peuvent commencer une session TLS :

S: <attend la connexion sur l'accès TCP 25>
C: <ouvre la connexion>
S: 220 mail.imc.org SMTP service prêt
C: EHLO mail.example.com
S: 250-mail.imc.org vous souhaite la bienvenue
S: 250-8BITMIME
S: 250-STARTTLS
S: 250 DSN
C: STARTTLS
S: 220 Continuer
C: <commence la négociation TLS>
C & S: <négocie une session TLS>
C & S: <vérifie le résultat de la négociation>
C: EHLO mail.example.com
S: 250-mail.imc.org vous salue bien
S: 250-8BITMIME
S: 250 DSN

6. Considérations sur la sécurité

On devrait noter que SMTP n'est pas un mécanisme de bout en bout. Donc, si une paire client/serveur SMTP décide d'ajouter la confidentialité TLS, ils ne sécurisent pas le transport entre l'agent d'utilisateur de messagerie d'origine et le receveur. De plus, comme la livraison d'un seul élément de messagerie peut passer entre plus de deux serveurs SMTP, ajouter la confidentialité TLS à une paire de serveurs ne signifie pas que la chaîne SMTP toute entière a été rendue confidentielle. De plus, juste parce que un serveur SMTP peut authentifier un client SMTP, cela ne signifie pas que les messages provenant du client SMTP ont été authentifiés par le client SMTP lorsque le client les a reçus.

Le client et le serveur SMTP doivent tous deux vérifier le résultat de la négociation TLS pour voir si un degré acceptable d'authentification et de confidentialité a été réalisé. Ignorer cette étape invalide complètement l'utilisation de TLS pour la sécurité. La décision sur la réalisation d'une authentification ou confidentialité acceptable est prise localement, dépend de la mise en œuvre, et sort du domaine d'application du présent document.

Le client et le serveur SMTP devraient noter soigneusement le résultat de la négociation TLS. Si la négociation résulte en l'absence de confidentialité, ou si elle résulte en une confidentialité qui utilise des algorithmes ou des longueurs de clé qui sont réputés trop faibles, ou si l'authentification n'est pas assez bonne pour l'une ou l'autre partie, le client peut choisir de terminer la session SMTP avec une commande QUIT immédiate, ou le serveur peut choisir de ne pas accepter d'autre commande SMTP.

Une attaque par interposition peut être lancée en supprimant la réponse "250 STARTTLS" du serveur. Cela va amener le client à ne pas essayer de commencer une session TLS. Une autre attaque par interposition est de permettre au serveur d'annoncer sa capacité STARTTLS, mais d'altérer la demande du client de commencer TLS et la réponse du serveur. Pour se défendre contre de telles attaques, client et serveur DOIVENT tous deux être capables d'être configurés à exiger une négociation TLS réussie d'une suite de chiffrement appropriée pour les hôtes choisis avant que les messages puissent être transférés. L'option supplémentaire d'utilisation de TLS lorsque possible DEVRAIT aussi être fournie. Une mise en œuvre PEUT fournir la capacité d'enregistrer que TLS a été utilisé dans une communication avec un certain homologue et de générer un avertissement si il n'est pas utilisé dans une session ultérieure.

Si la négociation TLS échoue ou si le client reçoit une réponse 454, il doit décider que faire ensuite. Il y a trois choix principaux : continuer le reste de la session SMTP, réessayer TLS ultérieurement, ou abandonner et retourner le message à l'envoyeur. Si un échec ou une erreur se produit, le client peut supposer que le serveur peut être capable de négocier TLS à l'avenir, et devrait essayer de négocier TLS dans une session ultérieure, jusqu'à ce qu'une temporisation fixée localement arrive à expiration, moment auquel le client devrait retourner le message à l'envoyeur. Cependant, si le client et le serveur n'utilisent TLS que pour l'authentification, le client peut vouloir continuer la session SMTP, au cas où certaines des opérations que le client voulait effectuer seraient acceptées par le serveur même si le client n'est pas authentifié.

Avant que commence la prise de contact TLS, toutes les interactions de protocole sont effectuées en clair et peuvent être modifiées par un attaquant actif.

Pour cette raison, clients et serveurs DOIVENT éliminer, à l'achèvement de la prise de contact, toutes les informations obtenues avant le début de cette prise de contact TLS.

L'extension STARTTLS ne convient pas pour l'authentification de l'auteur d'un message électronique sauf si chaque bond de la chaîne de livraison, y compris la soumission au premier serveur SMTP, est authentifié. Une autre proposition [RFC2554] peut être utilisée pour authentifier la livraison, et les multiparties de sécurité MIME [RFC1847] peuvent être utilisées pour authentifier l'auteur d'un message électronique. De plus, la proposition de la [RFC2554] offre des options plus simples et plus souples pour authentifier un client SMTP et le mécanisme SASL EXTERNAL [RFC2222] PEUT être utilisé conjointement avec la commande STARTTLS pour fournir une identité d'autorisation.

7. Références

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC2034] N. Freed, "Extension de service SMTP pour le retour de codes d'erreur améliorés", octobre 1996. *(P.S.)*

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2476] R. Gellens, J. Klensin, "Soumission de message", décembre 1998. (*Obsolète, voir* RFC4409) *(P.S.)*

[RFC2554] J. Myers, "Extension de service SMTP pour l'authentification", mars 1999. (*Obsolète, voir* RFC4954) *(P.S.)*

[RFC2821] J. Klensin, éditeur, "Protocole simple de transfert de messagerie", STD 10, avril 2001. *(Obsolète, voir* RFC5321*)*

Appendice Changements par rapport à la RFC 2487

Le présent document est une révision de la RFC2487, qui est une proposition de norme. Les changements par rapport à ce document sont :

- Section 5 et 7 : développement de l'exposé sur les attaques par interposition.
- Section 5 : développement de l'exposé sur quand un serveur devrait ou non annoncer l'extension STARTTLS.
- Section 5 : Changement des exigence pour le client SMTP à réception d'une réponse 220.
- Paragraphe 5.1 : Précisions à la description de la vérification des certificats.
- Paragraphe 5.3 : Ajout du paragraphe sur "STARTTLS sur l'accès de soumission".
- Section 6 : Correction d'une erreur dans l'exemple pour indiquer que le client doit produire une nouvelle commande EHLO, comme déjà décrit au paragraphe 5.2.
- Section 7 : Précisions au paragraphe sur le degré de confidentialité acceptable. Changement significatif à l'exposé sur comment éviter les attaques par interposition.
- Section 7 : Mise à jour de la référence de la RFC0821 en RFC2821.

Adresse de l'auteur

Paul Hoffman
Internet Mail Consortium
127 Segre Place
Santa Cruz, CA 95060
USA
téléphone : (831) 426-9827
mél : phoffman@imc.org

Déclaration complète de droits de reproduction

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