Groupe de travail Réseau
Request for Comments : 2505
BCP : 30
Catégorie : Bonnes pratiques actuelles

G. Lindberg, Chalmers University of Technology
février 1999
Traduction Claude Brière de L'Isle

Recommandations contre les pourriels pour les MTA SMTP

Statut de ce mémoire
Le présent mémoire apporte des informations à 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.

Résumé
Le présent mémoire fait un certain nombre de recommandations de mise en œuvre pour que les agents de transfert de messagerie (MTA, *Mail Transfer Agent*) du protocole simple de transfert de messagerie (SMTP, *Simple Mail Transfer Protocol*) [RFC0821], par exemple, d'envoi de messagerie, [SENDMAIL]) pour les rendre plus capables de réduire l'impact du spam(*).

* Spam (R) (avec une majuscule) est une marque commerciale déposée d'un produit alimentaire fait par Hormel. L'utilisation du terme spam (sans majuscule) dans la communauté de l'Internet vient d'une scénette des Monty Python et est presque du folklore de l'Internet. Le terme spam est habituellement péjoratif, cependant il n'est en aucune façon destiné à décrire le produit de Hormel.

L'objectif est que les présentes recommandations aident à nettoyer la situation des pourriels, si elles sont appliquées sur suffisamment de MTA SMTP sur l'Internet, et qu'elles devraient être utilisées comme lignes directrices pour les différents fabricants de MTA. Nous sommes parfaitement conscients que cette solution n'est pas la solution finale, mais si ces recommandations sont incluses, et utilisées, sur tous les MTA SMTP de l'Internet, les choses pourraient s'améliorer considérablement et donner du temps pour concevoir une solution à plus long terme. La section Travaux futurs suggère quelques idées qui pourront participer à une telle solution à long terme. Il se pourrait cependant très bien que la solution ultime soit sociale, politique, ou légale, plutôt que de nature technique.

Les mises en œuvre devraient être conscientes du risque accru d'attaques de déni de service auquel pourraient conduire plusieurs des méthodes proposées. Par exemple, un nombre accru d'interrogations des serveurs du système des noms de domaine (DNS, *Domain Name System*) et une taille accrue des fichiers de journalisation pourraient tous deux conduire à surcharger les systèmes et à des défaillances système durant une attaque.

Un bref résumé du présent mémoire dit :
- o Arrêter de relayer la messagerie non autorisée.
- o Les envoyeurs de pourriels devront alors opérer en plein jour ; traiter avec eux.
- o Concevoir un système de messagerie qui puisse traiter les pourriels.

1. Introduction

Le présent mémoire est une RFC des bonnes pratiques actuelles (BCP, *Best Current Practice*). À ce titre il devrait être utilisé comme lignes directrices pour les mises en œuvre de MTA SMTP pour rendre leurs produits plus capables d'empêcher/traiter les pourriels. Bien que cela soit son but principal, un effet collatéral voulu est de suggérer à la communauté des administrateurs système/maîtres de poste quels "trucs anti spam" est supposé avoir un MTA SMTP.

Le présent mémoire n'est cependant pas généralement destiné à faire une description de la façon de faire fonctionner un MTA SMTP - quels "trucs" mettre en œuvre et comment configurer les options. Si des suggestions sont fournies, elles seront clairement marquées et elles devront être lues comme telles.

1.1 Fondements

La messagerie électronique non sollicitée de masse, souvent connue sous le nom de pourriel (spam(*)), a considérablement augmenté depuis peu de temps et est devenue une menace sérieuse pour la communauté de la messagerie électronique de

l'Internet dans son ensemble. Il faut très vite faire quelque chose.

Le problème a plusieurs composants :

- C'est un gros volume, c'est-à-dire que les gens reçoivent des quantités de ces messages dans leurs boîtes aux lettres.
- C'est complètement "aveugle", c'est-à-dire, il n'y a pas de corrélation entre les centres d'intérêt du receveur et les messages envoyés (au moins si on suppose que sur l'Internet tout le monde n'est pas intéressé par les photographies pornographiques et les programmes de pourriels...).
- Cela coûte de l'argent aux receveurs. Comme de nombreux receveurs payent à leur fournisseur d'accès Internet (FAI) téléphonique le temps de transfert de leur boîte aux lettres à leur ordinateur, cela leur coûte réellement de l'argent.
- Cela coûte de l'argent au FAI. Supposons qu'un message de 10 koctets est envoyé à 10 000 usagers sur leur boîte aux lettres chez un FAI hôte ; cela signifie une mémorisation non sollicitée, non attendue de 100 Moctets. Les disques actuels, de 4 Goctets, peuvent prendre 40 flux de tels messages avant d'afficher complet. Il est presque impossible de planifier de telles "tempêtes".
- Beaucoup des envoyeurs de pourriels sont malhonnêtes, par exemple, se cachent derrière de fausses adresses de retour, écrivent délibérément des messages qui font croire qu'il s'agit d'un échange entre deux individus afin que le receveur du pourriel pense que c'est juste une erreur d'acheminement qui l'a fait arriver chez lui, disant que le message est "le matériel que vous avez demandé" alors que vous n'avez rien demandé, et font généralement tout ce que réprouve l'honnêteté et la morale pour essayer que quelques personnes de plus regardent leur message.
  En fait certains des programmes de pourriels mettent leur fierté à ajouter de fausses informations qui vont faire que les fournisseurs de service se grattent la tête.
  Il est courant que les gens qui protestent (souvent selon les instructions contenues dans le message) voient leur adresse de messagerie ajoutée à plus de listes de pourriels et vendues à des tiers.
- Il est de pratique assez courante d'utiliser des hôtes tiers comme relais pour obtenir l'envoi des pourriels aux receveurs. Ce vol de service est illégal dans la plupart – sinon tous – des pays (au moins les envoyeurs de pourriels américains ont été poursuivis en justice avec succès). Cependant, avec l'envoyeur original aux USA, le relais (innocent) en Suède et la liste des receveurs aux USA, le processus judiciaire pour obtenir des dommages et intérêts de la part des envoyeurs de pourriels devient extrêmement difficile.

1.2 Domaine d'application

Le présent mémoire n'envisage pas d'être la solution finale du problème du pourriel.

Cependant, si suffisamment de MTA de l'Internet mettent en œuvre un certain nombre des règles décrites ci-dessous (en particulier les règles de non relais) cela ferait sortir du bois les envoyeurs de pourriels et on pourrait s'occuper d'eux. Soit on peut s'appuyer sur des actions purement légales, soit on peut les bloquer de façon technique en utilisant les autres règles décrites ci-dessous (car les règles de non relais les font maintenant apparaître à découvert, avec leurs propres hôtes et domaines, on peut appliquer divers filtres d'accès contre eux). En réalité, une combinaison de méthodes légales et techniques va vraisemblablement donner les meilleurs résultats.

De cette façon, le problème du pourriel pourrait être suffisamment réduit pour permettre à la communauté de l'Internet de concevoir et déployer une réelle solution générale.

Mais, notez s'il vous plaît que les règles de non relais ne sont pas suffisantes par elles-mêmes pour stopper le pourriel. Même si 99 % des MTA SMTP les mettent en œuvre à partir du jour J, les envoyeurs de pourriels pourront encore trouver les 1 % restants et les utiliser. Ou les envoyeurs de pourriels vont juste changer de vitesse et se connecter directement à chaque hôte receveur ; cela va coûter plus cher à l'envoyeur de pourriels, mais c'est assez probable.

Même si le déploiement de IPv6 est proche, le problème du pourriel est déjà là et donc le présent mémoire se restreint au problème actuel de IPv4.

1.3 Terminologie

Dans le présent mémoire, on va utiliser la terminologie de la [RFC2119] :

- "DOIT" : ce mot ou l'adjectif "EXIGÉ" signifie que cet élément est une exigence absolue.
- "DEVRAIT" : ce mot ou l'adjectif "RECOMMANDÉ" signifie qu'il peut exister des raisons valides dans des circonstances particulières pour ignorer cet élément, mais toutes les implications en devraient être soigneusement étudiées et le cas devrait être évalué avec soin avant de choisir une voie différente.
- "PEUT" : ce mot ou l'adjectif "FACULTATATIF" signifie que cet élément est vraiment facultatif. Un fabricant peut choisir d'inclure l'élément parce que, par exemple, un marché particulier l'exige ou parce qu'il améliore le produit ; un autre fabricant peut omettre le même élément.

1.4 Utilisation des informations du DNS

Dans le présent mémoire, on utilise parfois le terme "nom d'hôte" ou "nom de domaine" qui devrait être interprété comme un nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*). On entend par là le nom retourné par le DNS en réponse à une interrogation PTR (.IN-ADDR.ARPA) c'est-à-dire lorsque une adresse IP est traduite en un nom, ou bien on entend un nom avec un enregistrement DNS A ou MX associé ; [RFC1034] et [RFC1035].

Lorsque on suggère d'utiliser des FQDN plutôt que des adresses IP, c'est parce que les FQDN sont intuitivement plus faciles à utiliser. Cependant, un tel usage dépend largement des informations du DNS et de .IN-ADDR.ARPA (PTR). Comme il est très facile de falsifier cela, soit par des informations d'antémémoire falsifiées injectées dans les serveurs du DNS, soit par des envoyeurs de pourriels qui font leur propre DNS avec de fausses informations, les noms d'hôtes et de domaines doivent être utilisés avec précaution, par exemple en vérifiant que la traduction adresse->nom correspond à celle de nom->adresse. Avec le DNS sécurisé, [RFC2065], les choses vont s'améliorer, car l'usurpation d'identité dans .IN-ADDR.ARPA ne sera plus possible.

Une des recommandations est sur la vérification des domaines "MAIL From:" (générateur de l'enveloppe) auprès du DNS (qui assure que les informations DNS appropriées existent pour le domaine). Lorsque on utilise cette capacité, il faut prendre quelques éléments en considération :

(1) On ne doit pas oublier l'augmentation du nombre d'interrogations du DNS qui peut résulter en problèmes pour le serveur DNS lui-même pour faire face à la charge. Cela peut par lui-même déboucher sur une attaque de déni de service contre le serveur DNS juste par l'envoi de messages électroniques à un site.

(2) On devrait noter qu'avec la mise en antémémoire négative dans le DNS, des réponses DNS falsifiées peuvent être utilisées pour monter des attaques de déni de service. Par exemple, si un site est connu pour mettre en œuvre une vérification de validité de FQDN sur les adresses dans les commandes SMTP "MAIL From:", un attaquant peut être capable d'utiliser les réponses négatives du DNS pour bloquer effectivement l'acceptation de messages d'une ou plusieurs origines. À cause de cela, on devrait vérifier avec soin le serveur DNS utilisé, par exemple, comment il vérifie que les réponses entrantes correspondent aux interrogations en cours, pour minimiser le risque de telles attaques.

(3) Pour les premières versions de logiciels de pourriels, les vérifications des FQDN donnent un peu de répit, car ce logiciel génère un "MAIL From:" complètement faux qui ne va jamais rentrer dans le système si il est vérifié par le DNS. Cela est utilisé activement aujourd'hui dans de nombreuses installations et cela réduit effectivement les pourriels.

D'un autre côté, les sites qui ont une faible connexité au DNS peuvent trouver que leur messagerie légitime a des problèmes pour joindre des destinations à cause des temporisations du DNS lorsque les receveurs vérifient leur "MAIL From:". Cependant, comme les informations du DNS sont traitées en asynchrone et sont mises en antémémoire même si le demandeur initial a abandonné, il y a de fortes chances pour que les informations nécessaires soient là lors d'une tentative ultérieure.

Pour les plus récentes versions du logiciel de pourriels, une vérification de "MAIL From:" va probablement être moins utile, car les logiciels de pourriel évoluent aussi et vont commencer à utiliser les adresses de messagerie existantes (il sort du domaine d'application du présent mémoire de dire si cela est légal ou non). Mais, au moins, l'Internet bénéficiera de l'effet collatéral d'arrêter par cet essai les erreurs typographiques et les agents d'utilisateur (UA, *User Agent*) mal configurés.

1.5 Où bloquer les pourriels, dans SMTP, dans la RFC822 ou dans l'UA

Notre hypothèse de base est que le refus/acceptation est traité à la couche SMTP et qu'un MTA qui décide de refuser un message devrait le faire lorsque il est encore dans le dialogue SMTP. D'abord, cela signifie qu'on n'a pas à mémoriser une copie d'un message qu'on va ultérieurement décider de refuser, et ensuite, notre responsabilité pour ce message est faible ou nulle – car on ne l'a pas encore lu ; on laisse à l'envoyeur le soin de réparer l'erreur.

1.6 Codes de retour SMTP

SMTP a plusieurs classes de codes de retour, voir l'exposé de la [RFC0821] :

- 5xx est une réponse de non réalisation permanente (erreur fatale) et résulte en la fin du transfert de message, et au retour du message à l'envoyeur.
- 4xx est une réponse de non réalisation transitoire (erreur temporaire) et résulte en le retour du transfert du message dans la file d'attente et en un nouvel essai ultérieurement.
- 2xx est une réponse d'achèvement positive et indique que le MTA a maintenant pris la responsabilité de la livraison du message.

Lorsque on utilise les options/"trucs" décrits dans le présent mémoire, certaines choses sont à prendre en considération :

Pour certains événements, comme "Refusé – vous êtes sur la liste des envoyeurs de pourriels", 5xx peut être le code de retour correct, car cela termine immédiatement la session et on en a fini avec lui (en supposant que l'envoyeur de pourriel joue selon les règles de SMTP, ce qu'il peut décider de ne pas faire – en fait il peut remettre le pourriel dans la file d'attente, sans considération pour le code de retour. Cependant, une erreur 5xx dans une mauvaise configuration peut être cause du rejet d'un message légitime, ce qui peut être assez malheureux.

Donc, on suggère un 4xx comme code de retour pour la plupart des cas. Comme c'est une erreur non fatale, le message est remis en file d'attente chez l'envoyeur et on a au moins un peu de temps pour découvrir et corriger les erreurs de configuration, plutôt que d'avoir des messages rejetés (normalement, cela arrive lorsque on refuse de relayer pour les domaines qu'on devrait en fait accepter car on est sur leur liste MX).

Une réponse 4xx amène aussi l'hôte de l'envoyeur de pourriels à remettre le message en file d'attente et si c'est réellement son propre hôte qui l'obtient, c'est probablement une bonne chose – cela remplit son disque avec ses propres pourriels. Si, d'un autre côté, il utilise quelqu'un d'autre comme hôte relais, tous ces pourriels mis en file d'attente sont une très bonne preuve que quelque chose va de travers et cela devrait attirer l'attention de cet hôte relais.

Cependant, un code 4xx Erreur temporaire peut avoir une interaction inattendue avec les enregistrements MX. Si le domaine receveur a plusieurs enregistrements MX et que l'hôte du MX de moindre préférence refuse de recevoir des messages avec un code de réponse "451", l'hôte envoyeur peut choisir, et il va souvent le faire, d'utiliser l'hôte suivant sur la liste MX. Si l'hôte MX suivant n'a pas la même liste de refus, il va bien sûr vouloir accepter le message, seulement pour trouver que l'hôte final refuse encore de recevoir ce message ("MAIL From:"). Notre intention était de faire rester le message délictueux chez l'hôte de l'auteur du délit et qu'il remplisse son disque de file d'attente mqueue, mais tout cela aboutit chez notre ami, le prochain hôte au MX de moindre préférence.

Finalement, il a été suggéré qu'on puisse utiliser un code de retour 2xx mais néanmoins décider de ne pas transmettre ou recevoir les pourriels ; les solutions de remplacement normales sont de les mémoriser ailleurs (par exemple, /dev/null). Cela viole clairement les intentions de la [RFC0821] et ne devrait pas être fait sans de très grandes précautions – au lieu d'éliminer aveuglément les messages, on pourrait les remettre en file d'attente et les inspecter manuellement (ou automagiquement) pour voir si c'est du pourriel ou de la messagerie légitime et si ils devraient être éliminés ou transmis.

1.7 Listes de diffusion

Un MTA qui a aussi la capacité de traiter les listes de diffusion et de les étendre à un certain nombre de receveurs, doit être capable d'autoriser les envoyeurs et de protéger ses listes contre les pourriels. Les mécanismes pour ce faire peuvent être très différents de ceux utilisés pour la messagerie et les usagers ordinaires et ne sont pas traités dans le présent mémoire.

2. Recommandations

On donne ici une brève liste de recommandations, suivie par une discussion plus détaillé de chacune d'elles. On va aussi donner des recommandations sur des choses à NE PAS FAIRE, des choses qui peuvent sembler naturelles dans la lutte contre les pourriels (et qui peuvent même fonctionner dans une certaine mesure) mais peuvent avoir un effet ravageur sur la messagerie Internet et donc causer plus de mal que de bien.

1) DOIT être capable d'interdire l'utilisation non autorisée comme relais de messagerie.
2) DOIT être capable de fournir suffisamment d'informations dans les lignes "Received:" pour rendre possible le traçage du chemin du message, en dépit de l'utilisation de noms d'hôtes falsifiés dans les déclarations de HELO, etc., par les envoyeurs de pourriels.
3) DOIT être capable de fournir des informations de journalisation locale qui rendent possible de retracer les événements après coup.
4) DEVRAIT être capable d'enregistrer dans la journalisation toutes les occurrences d'actions anti-relais/anti-pourriel.
5) DEVRAIT être capable de refuser la messagerie provenant d'un hôte ou groupe d'hôtes.

6a) NE DOIT PAS refuser "MAIL From: <>".
6b) NE DOIT PAS refuser "MAIL From: <user@my.local.dom.ain>".
7a) DEVRAIT être capable de refuser les messages provenant d'un usager "MAIL From:" spécifique, <foo@domain.example>.
7b) DEVRAIT être capable de refuser les messages provenant d'un domaine "MAIL From:" <.*@domain.example> entier.

8) DEVRAIT être capable de limiter le flux de messages ("Contrôle du débit").
9) DEVRAIT être capable de vérifier le domaine "MAIL From:" (en utilisant le DNS ou d'autres moyens).
10) DEVRAIT être capable de vérifier <local-part> dans la messagerie sortante.

11) DEVRAIT être capable de contrôler VRFY et EXPN de SMTP.
12) DEVRAIT être capable de contrôler l'ETRN de SMTP.
13) DOIT être capable de se configurer à fournir des codes de retour différents pour des règles différentes (par exemple 451 Erreur temporaire par opposition à 550 Erreur fatale).

L'exposé ci-dessous se termine souvent par le besoin de diverses formes de correspondance à un gabarit sur les noms de domaine/hôte et les adresses/sous réseaux IP. Il est RECOMMANDÉ que les données/gabarit pour ce faire PUISSENT être fournis en dehors du MTA, par exemple que les règles de correspondance au gabarit soient incluses dans le MTA mais que les schémas réels PUISSENT être dans un fichier externe. Il est aussi RECOMMANDÉ que les règles de correspondance au gabarit (fichier externe) PUISSENT contenir des expressions régulières, pour donner un maximum de souplesse.

Bien sûr, la correspondance de chaînes sur les noms de domaine/hôte NE DOIT PAS être sensible à la casse. Comme <local-part> PEUT être sensible à la casse, il PEUT être naturel de conserver cela ici. Cependant, comme <sPAmMeR@domain.example> et <spammer@domain.example> est très probablement le même usager et comme les comparaisons de chaînes sont utilisées pour refuser ses messages, on suggère que les comparaisons de <local-part> soient aussi insensibles à la casse.

L'interprétation qui DEVRAIT s'appliquer à toutes ces recommandations est la souplesse – sans considération de la façon dont nous concevons aujourd'hui les règles anti-pourriels, les envoyeurs de pourriels trouveront le moyen de les contourner et un MTA bien conçu DEVRAIT être assez souple pour répondre à ces nouvelles menaces.

2.1 Interdire les usages de relais de messagerie non autorisés

L'utilisation non autorisée d'un hôte comme relais de messagerie est un vol des ressources du relais et met en danger la réputation du propriétaire du relais. Elle rend aussi impossible de filtrer ou bloquer les pourriels sans en même temps bloquer la messagerie légitime.

Donc, le MTA DOIT être capable de contrôler/refuser un tel usage de relais.

Dans une session SMTP on a quatre éléments, dont chacun a un degré de confiance différent :

1) "Nom d'hôte du HELO" facilement et souvent falsifié.
2) "MAIL From:" facilement et souvent falsifié.
3) "RCPT To:" correct, ou au moins prévu.
4) SMTP_Caller (hôte) adresse de source IP OK, FQDN PEUT être OK.

Comme 1) et 2) sont si facilement et si souvent falsifiés, on ne peut pas du tout s'appuyer sur eux pour autoriser l'usage de notre hôte comme relais de messagerie.

Au lieu de cela, le MTA DOIT être capable d'autoriser l'usage comme relais de messagerie sur la base d'une combinaison de :

- l'adresse (domaine) "RCPT To:".
- nom d'hôte FQDN SMTP_Caller.
- l'adresse IP du SMTP_Caller.

L'algorithme suggéré est :

a) Si "RCPT To:" est un de "nos" domaines, local ou un domaine auquel on accepte de transmettre (MX de remplacement), on accepte alors de relayer.
b) Si SMTP_Caller est autorisé, soit à son adresse IP de source, soit son FQDN (selon que l'on fait ou non confiance an DNS) on accepte de relayer.
c) Autrement, on refuse de relayer.

Lorsque on fait a) on doit s'assurer que toutes les sortes d'acheminement de source SMTP (aussi bien le chemin officiel [@a,@b:u@c], que le taxi '%' et le '!' de style uucp) est soit complètement supprimé avant l'essai, soit est au moins pris en compte.

Un site qui met en œuvre cette exigence DOIT aussi être conscient que cela peut bloquer des messages correctement adressés, en particulier ceux qui sont générés ou qui se terminent dans une passerelle avec un système de messagerie différent de SMTP. Avant de mettre en œuvre une telle politique, un inventaire soigneux DEVRAIT être fait pour s'assurer que tous les algorithmes d'acheminement utilisés, soit par les autres systèmes de messagerie, soit ad hoc, sont connus. Chacun de ces systèmes DOIT être traité au cas par cas.

Un exemple d'un tel système de messagerie, et de son schéma d'adressage est X.400 avec une adresse du type :

"/c=us/admd= /prmd=xyz/dd.rfc-822=usager(a)final/"@passerelle-x400

Un autre exemple est celui du MAIL-11 de DECnet, qui peut avoir des adresses de la forme :

"passerelle::smtp%\"usager@final\""@passerelle-mail-11

Dans tous les cas, la configuration DOIT accepter les caractères génériques pour les FQDN et les adresses IP à classe pleine et DEVRAIT accepter "adresse/gabarit" pour les adresses IP sans classe, par exemple domain.example et *.domain.example ; 10.11.*.*, 192.168.1.*, 192.168.2.*, 10.0.0.0/13, 192.168.1.0/23.

La configuration DEVRAIT permettre que les données de décision/gabarit soient fournies par une source externe, par exemple un fichier texte ou une base de données dbm. La décision/gabarit DEVRAIT être autorisée à contenir des expressions régulières.

2.2 Ligne Received:

Le MTA DOIT ajouter une ligne "Received:" devant le message (comme décrit dans la [RFC0822], et exigé dans la [RFC1123]). Cette ligne "Received:" DOIT contenir assez d'informations pour rendre possible le traçage du chemin de retour du message à l'envoyeur. On a deux cas :

2.2.1 Connexion directe de MTA à MTA

La messagerie Internet a été conçue de telle sorte que l'hôte qui envoie se connecte directement au receveur, comme décrit par les enregistrements MX (il PEUT y avoir plusieurs hôtes MX sur une liste de priorités). Pour assurer la traçabilité du retour vers l'hôte envoyeur (qui PEUT être un pare-feu/passerelle, comme décrit plus loin) chaque MTA le long du chemin, y compris le MTA final, DOIT ajouter devant une ligne "Received:". Pour une telle ligne "Received:" :
elle DOIT contenir :
- l'adresse IP de l'appelant ;
- la 'date-heure' comme décrit à la page 18 de la [RFC0822] ;

elle DEVRAIT contenir :
- le FQDN correspondant à l'adresse IP de l'appelant ;
- l'argument donné dans la déclaration de "HELO" ;
- les informations d'authentification, si une connexion authentifiée a été utilisée pour la transmission/soumission.

Il est suggéré que la plupart des autres champs "Received:" décrits dans la [RFC0822] soient inclus dans les lignes "Received:".

Fondamentalement, toute information qui peut aider à retracer le message peut et DEVRAIT être ajoutée à la ligne "Received:". Cela est vrai même lorsque la soumission initiale est non SMTP, par exemple une soumission via un client de messagerie fondé sur la Toile où http est utilisé entre le client et le serveur de la Toile, une ligne "Received:" peut être utilisée pour identifier cette connexion, déclarant que l'adresse IP a été utilisée lors de la connexion au serveur http où le message a été créé.

Ces recommandations sont délibérément plus fortes que celles de la [RFC1123], et sont là pour assurer que le message envoyé directement d'un hôte envoyeur de pourriels à un receveur peut être tracé avec une précision suffisante ; un bon exemple est celui d'un envoyeur de pourriels qui utilise un compte téléphonique : le FAI a besoin d'avoir son adresse IP à la 'date-heure' pour être capable de prendre des mesures contre lui.

2.2.2 Appareils de type pare-feu/passerelle

Les organisations qui ont pour politique de dissimuler la structure interne de leur réseau DOIVENT quand même être autorisées à, et capables de, faire ainsi. Elles font généralement ajouter à leurs MTA internes des lignes "Received:" avec une quantité d'informations très limitée, ou n'ajoutent rien du tout. Elles envoient ensuite leurs messages à travers une sorte d'appareil pare-feu/passerelle, qui PEUT même retirer toutes les lignes "Received:" des MTA internes avant d'ajouter ses propres lignes"Received:" (comme exigé dans la [RFC1123]).

En faisant ainsi, elles prennent la pleine responsabilité de la traque des envoyeurs de pourriels qui envoient de l'intérieur de leur organisation ou bien elles acceptent d'être tenues pour responsables de ces activités d'envoi de pourriels. Il est EXIGÉ que les informations fournies dans leurs messages sortants soient suffisantes pour qu'elles effectuent tout le traçage nécessaire.

Dans le cas de messages entrants dans une organisation, les lignes "Received:" DOIVENT être gardées intactes pour s'assurer que les usagers qui reçoivent des messages de l'intérieur puissent donner les informations nécessaires pour retracer les messages entrants jusqu'à leur origine.

Généralement, une passerelle NE DEVRAIT PAS changer ou supprimer les lignes "Received:" à moins qu'il y ait une exigence de sécurité pour le faire. Changer le contenu des lignes "Received:" existantes pour s'assurer que "elles ont un sens" lorsque elle traversent une passerelle de messagerie détruit souvent d'une certaine façon et supprime les informations nécessaires pour rendre un message traçable. Il faut veiller à préserver les informations des lignes "Received:", soit dans le message lui-même, le message qu'obtient le receveur, soit si c'est impossible, dans les fichiers de journalisation.

2.3 Journalisation d'événements

Le MTA DOIT être capable de fournir assez d'informations de journalisation locale pour rendre possible la trace des événements. Cela inclut la plupart des informations mises dans les lignes "Received:" ; voir ci-dessus.

2.4 Actions de journalisation anti-relais/anti-pourriels

Le MTA DEVRAIT être capable d'enregistrer toutes les actions anti-relais/anti-pourriels. Les entrées d'enregistrement DEVRAIENT contenir au moins :

- les informations d'heure.
- les information sur le refus, c'est-à-dire, pourquoi la demande a été refusée ("Mail From", "Relais refusé", "Envoyeur de pourriels", "Hôte de pourriels", etc.).
- les adresses (domaines) "RCPT To:"). (Si la connexion a été interdite antérieurement, par exemple lors de la vérification de l'adresse IP SMTP_Caller, l'adresse "RCPT To:" est inconnue et donc ne peut être enregistrée.)
- l'adresse IP de l'hôte incriminé.
- le nom d'hôte FQDN de l'hôte incriminé.
- les autres informations pertinentes (par exemple, données pendant le dialogue SMTP, avant la décision de refus de la demande).

On DEVRAIT noter qu'en enregistrant plus d'événements, en particulier les messages refusés, on ouvre la possibilité d'attaques de déni de service, par exemple en remplissant les journaux avec une très grande quantité de commandes "RCPT To:". Une mise en œuvre qui se lance dans l'enregistrement selon la présente description DOIT être consciente du fait que la taille des fichiers de journalisation augmente particulièrement pendant les attaques.

2.5 Refuser les messages sur la base de l'adresse SMTP_Caller

Le MTA DEVRAIT être capable d'accepter ou refuser les messages provenant d'un hôte ou groupe d'hôtes spécifique. On veut dire ici l'adresse IP de source ou le FQDN en lequel son .IN-ADDR.ARPA se résout (selon que l'on fait ou non confiance au DNS). Cette fonctionnalité pourrait être mise en œuvre à un pare-feu, mais comme le MTA DEVRAIT être capable de se "défendre lui-même", on recommande qu'il soit capable aussi de cela.

Il est RECOMMANDÉ que le MTA soit capable de décider sur la base des noms d'hôte FQDN (host.domaine.exemple), sur des noms de domaine avec caractère générique (*.domaine.exemple), sur des adresses IP individuelles (10.11.12.13) ou sur des adresses IP avec une longueur préfixée (10.0.0.0/8, 192.168.1.0/24).

Il est aussi RECOMMANDÉ que ces règles de décision puissent être combinées pour former une liste souple de accepte/refuse/accepte/refuse, par exemple :

```
accepte  host.domaine.exemple
refuse   *.domaine.exemple
accepte  10.11.12.13
accepte  192.168.1.0/24
refuse   10.0.0.0/8
```

La liste est parcourue jusqu'à ce qu'il y ait une première correspondance et l'action de accepte/refuse se fonde sur cela.

La longueur d'adresse IP est RECOMMANDÉE. Cependant, les mises en œuvre avec des caractères génériques, par exemple 10.11.12.* (seulement pour les réseaux à classe pleine sur les limites d'octet) sont bien sûr beaucoup mieux que ceux qui ne l'ont pas.

Pour améliorer encore plus le filtrage, le MTA PEUT fournir des expressions régulières complètes à utiliser pour les noms d'hôtes ; éventuellement aussi pour les adresses IP.

2.6 "MAIL From: <>" et "MAIL From: <user@my.local.dom.ain>"

Bien que la lutte contre les envoyeurs de pourriels soit importante, elle ne DOIT jamais être faite d'une façon qui viole les normes existantes de la messagerie électronique. Comme les envoyeurs de pourriels falsifient souvent les adresses "MAIL From:", il est tentant de mettre des restrictions générales sur ce champ, en particulier pour certaines adresses "évidentes". Cela PEUT, cependant, causer plus de dommages à la communauté de la messagerie que n'en causent les pourriels.

Lorsque il est nécessaire de refuser les messages provenant d'un certain hôte ou site, notre recommandation est d'utiliser d'autres méthodes mentionnées dans le présent mémoire, par exemple, de refuser les messages sur la base de l'adresse (ou nom) SMTP_Caller, sans considération du "MAIL From:" qui a été utilisé.

2.6.1 "MAIL From: <>"

Le MTA NE DOIT PAS refuser de recevoir "MAIL From: <>".

L'adresse "MAIL From: <>" est utilisée dans les messages d'erreur provenant du système de messagerie lui-même, par exemple, lorsque un relais de messagerie légitime est utilisé et renvoie un message d'erreur à l'usager. Refuser de recevoir un tel message signifie que les usagers NE PEUVENT PAS avoir de notification des erreurs de leur messagerie sortante, par exemple "Usager inconnu", ce qui sans nul doute cause plus de ravages dans la communauté de la messagerie que ne le font les pourriels.

Le cas le plus courant de tels "MAIL From: <>" légitimes est pour un receveur, c'est-à-dire, un message d'erreur retourné à un seul individu. Comme les envoyeurs de pourriels ont utilisé "MAIL From: <>" pour envoyer à de nombreux receveurs, il est tentant de rejeter complètement de tels messages ou de les rejeter tous sauf le premier receveur. Cependant, il y a des causes légitimes pour qu'un message d'erreur aille à plusieurs receveurs, par exemple une liste avec plusieurs propriétaires de la liste, tous situés sur le même site distant, et donc, le MTA NE DOIT PAS refuser "MAIL From: <>" même dans ce cas.

Cependant, le MTA PEUT mettre la connexion TCP au ralenti (fréquence de "read()") si il y a plus d'un "RCPT To:" et de cette façon ralentir les envoyeurs de pourriels qui utilisent "MAIL From: <>".

2.6.2 "MAIL From: <user@my.local.dom.ain>"

Le MTA NE DOIT PAS refuser "MAIL From: <user@my.local.dom.ain>".

Par "my.local.dom.ain" on veut dire le ou les noms de domaine qui sont traités comme locaux et résultent en une livraison locale. Au premier abord, il PEUT sembler que personne d'autre n'a besoin d'utiliser "MAIL From: <user@my.local.dom.ain>" et que des restrictions sur qui PEUT utiliser cela vont réduire le risque de fraude et donc réduire les pourriels. Bien que cela PUISSE être vrai à (très) court terme, cela exclut aussi au moins deux usages légitimes:

- o les alias (fichiers .forward) : <user1@my.local.dom.ain> envoie à <user2@external.example> et ce message est renvoyé à <user2@my.local.dom.ain>, par exemple si <user2> est parti à my.local.dom.ain et a un fichier .forward à external.example.
- o listes de diffusion : La [RFC1123] donne une exigence claire que "MAIL From:" pour les messages d'une liste de diffusion DEVRAIT refléter le propriétaire de la liste, plutôt que l'envoyeur individuel. À cause de ce fait, et du fait que le propriétaire de la liste pourrait n'être pas lui-même dans le même domaine que la liste (hôte de liste), des messages PEUVENT arriver au domaine du propriétaire de la liste (hôte de messagerie) à partir d'un domaine étranger (d'un hôte qui sert un domaine étranger) avec le domaine local du propriétaire de liste dans la commande in "Mail From:".

Si "MAIL From: <user@my.local.dom.ain>" est rejeté, ces deux cas vont donner des échec de livraison de messages légitimes.

2.7 Refus sur la base de "MAIL From:"

Le MTA DEVRAIT être capable de refuser de recevoir des messages d'un usager "MAIL From:" spécifique (foo@domain.example) ou d'un domaine "MAIL From:" entier (domain.example). En général, ces sortes de règles sont faciles à surmonter par les envoyeurs de pourriels qui changent de "MAIL From:" très souvent, mais la capacité à bloquer un certain usager ou un certain domaine est assez utile lorsque une attaque vient juste d'être découverte et est en cours.

Prière de noter que :

"MAIL From: <>"

et

"MAIL From: <user@my.local.dom.ain>"

NE DOIVENT PAS être refusés (voir ci-dessus) sauf lorsque d'autres politiques bloquent la connexion, par exemple lorsque l'adresse IP SMTP_Caller de l'homologue appartient à un réseau qui est délibérément refusé.

2.8 Contrôle du débit

Le MTA DEVRAIT fournir des outils pour que l'hôte de messagerie contrôle le débit auquel les messages sont envoyés ou reçus. L'idée comporte deux aspects :

1) Si on se trouve avoir un usager de messagerie légitime avec un compte existant légitime et si cet usager envoie des pourriels, on PEUT vouloir réduire sa vitesse d'envoi. Ceci est assez controversé et DOIT être utilisé avec d'extrêmes précautions, mais cela PEUT protéger le reste de l'Internet de ses agissements.
2) Si on subit une attaque de pourriels, cela PEUT nous aider considérablement d'être juste capable de ralentir le taux de messagerie entrante pour cet usager/hôte particulier.

Pour l'envoi de messagerie, cela a été fait en ralentissant la connexion TCP pour établir un taux de sortie de données acceptable, par exemple en réduisant la fréquence de "write()".

Pour la réception de messages, on pourrait utiliser fondamentalement la même technique, par exemple, réduire la fréquence de "read()", ou on pourrait signaler par un code de retour 4xx qu'on ne peut pas recevoir. Il est RECOMMANDÉ que la décision d'une telle action se fonde sur l'usager "MAIL From:", le domaine "MAIL From:", le SMTP_Caller (nom/adresse), "RCPT TO:", ou une combinaison de tous.

2.9 Vérifier "MAIL From:"

Le MTA DEVRAIT être capable d'effectuer une simple "vérification de bonne santé" du domaine "MAIL From:" et refuser de recevoir le message si ce domaine est non existant (c'est-à-dire, ne se résout pas en ayant un enregistrement MX ou A). Si l'erreur du DNS est temporaire, TempFail, le MTA DOIT retourner un code d'erreur 4xx (Erreur temporaire). Si l'erreur du DNS est un Authoritative NXdomain (hôte/domaine inconnu) le MTA DEVRAIT quand même retourner un code d'erreur 4xx (car ce PEUT juste être que le DNS principal et secondaire ne sont pas synchronisés) mais il PEUT permettre un code d'erreur de 5xx (comme configuré par l'administrateur de système).

2.10 Vérifier <local-part>

Le MTA DEVRAIT permettre que la <partie-locale> de la messagerie sortante soit vérifiée afin que le nom de l'envoyeur soit un usager réel ou un alias existant. Cela sert fondamentalement à protéger le reste de l'Internet contre diverses "erreurs typographiques". :

MAIL From: <fo0bar@domain.example>

et/ou d'utilisateurs malveillants

MAIL From: <Vous.ne.me.connaissez.pas@domain.example>

Comme toujours cela peut être outrepassé par les envoyeurs de pourriels qui veulent vraiment le faire, mais avec des règles plus strictes pour le relais, cela devient de plus en plus difficile. En fait, attraper les "erreurs typographiques" au relais de messagerie initial (et officiel) est en soi une motivation suffisante pour la présente recommandation.

2.11 VRFY et EXPN SMTP

VRFY et EXPN SMTP fournissent tous deux les moyens à un envoyeur potentiel de pourriels de vérifier si les adresses de sa liste sont valides (VRFY) et même d'obtenir plus d'adresses (EXPN). Donc, le MTA DEVRAIT contrôler à qui il est permis de produire ces commandes. Cela PEUT être "marche/arrêt" ou cela PEUT utiliser des listes d'accès similaires à celles mentionnées précédemment.

Noter que la commande "VRFY" est exigée conformément à la [RFC0821]. La réponse peut, cependant, être "252 Argument non vérifié" pour représenter "arrêt" ou être bloquée via une liste d'accès. Cela DEVRAIT être la valeur par défaut.

La valeur par défaut pour la commande "EXPN" DEVRAIT être "arrêt".

2.12 ETRN SMTP

ETRN SMTP signifie que le MTA va faire fonctionner à nouveau sa file d'attente de messagerie, ce qui PEUT être assez coûteux et ouvrir la voie à des attaques de déni de service. Donc, le MTA DEVRAIT contrôler à qui il est permis de produire une commande ETRN. Elle PEUT être "marche/arrêt" ou il PEUT utiliser des listes d'accès similaires à celles mentionnées précédemment. La valeur par défaut DEVRAIT être "arrêt".

2.13 Codes de retour

La principale question est ici celle de la souplesse – il n'est simplement pas possible de définir dans un document comment faire un compromis entre retourner 5xx et faire échouer directement des messages légitimes à cause d'une faute de configuration et retourner 4xx et être capable de rattraper de telles fautes de configuration via une inspection du fichier de journalisation.

Donc, le MTA DOIT être configurable de façon à fournir "Succès" (2xx), "Échec temporaire" (4xx) ou "Échec permanent" (5xx) pour des règles ou politiques différentes. Les codes de retour exacts, autres que le premier chiffre (2, 4 ou 5) DEVRAIENT, cependant, ne pas être configurables. Cela parce qu'il est facile de configurer le logiciel de travers, et du fait que le choix de exactement quel code d'erreur utiliser est très subtil et que de nombreuses mises en œuvre de logiciel vérifient en fait au delà du premier chiffre (2, 4 ou 5) dans le code de retour.

Cependant, lorsque la réponse est le résultat d'une recherche dans le DNS et que le système DNS a retourné une erreur temporaire, le MTA DOIT le refléter et fournir un code de retour 4xx. Si la réponse du DNS est un domaine NX d'autorité (hôte ou domaine inconnu) le MTA PEUT le refléter par un code de retour 5xx.

Prière de se référer à l'exposé précédent sur les codes de retour SMTP pour des informations complémentaires.

2.13.1 Importance de la souplesse - exemple

Á Chalmers University of Technology notre DNS contient

```
cdg.chalmers.se.   IN  MX    0   mail.cdg.chalmers.se.
                   IN  MX  100   mail.chalmers.se.
```

et de même pour la plupart des sous-domaines, c'est-à-dire qu'un second hôte pour mémoriser les messages pour chaque sous-domaine, pour si leur hôte de messagerie était en panne. Cela signifie que mail.chalmers.se DOIT être prêt à agir comme relais de messagerie pour les sous-domaines ("RCPT To:") qu'il dessert et que les hôtes de messagerie de ces sous-domaines doivent accepter les connexions SMTP provenant de mail.chalmers.se. Les dernières versions de logiciels d'envoi de pourriels se servent de ce fait en utilisant toujours mail.chalmers.se pour livrer leurs messages à nos sous-domaines et ce faisant, elles obtiennent le relais de messagerie pour eux et ils empêchent les hôtes receveurs de refuser les connexions SMTP sur la base de l'adresse IP ou du FQDN de l'hôte envoyeur.

Tant que nous conservons notre concept d'avoir un hôte MX secondaire, nous ne pouvons pas réellement faire que mail.chalmers.se refuse le relais de messagerie, au moins avec un code de retour de 5xx. Cependant, il a été très facile d'identifier les hôtes/domaines/réseaux qui utilisent cette possibilité et de refuser d'agir comme relais de messagerie pour eux – et seulement eux – et de faire cela avec un code retour de 4xx. La messagerie légitime provenant d'eux PEUT être retardée si l'hôte receveur final est en panne mais elle sera finalement livrée lorsque il sera rétabli (code de retour 4xx) et cela n'est pas pire que si nous avions changé notre conception de MX. Les pourriels reçoivent maintenant une réponse "Refusé" et doivent se connecter à chacun des receveurs, qui PEUVENT décider de refuser la connexion SMTP.

Le minimum est que ceci est rendu possible parce que 1) il y a assez de souplesse dans le code d'autorisation de relais et 2) assez de souplesse dans l'assignation des codes de retour – un MTA avec un code de retour 5xx gravé dans le marbre aurait rendu cela absolument impossible.

3. Travaux futurs

3.1 Impact sur les UA SMTP et sur les utilisateurs finaux

Bien que le présent mémoire soit sur les MTA et fasse des recommandations pour eux, une partie de son contenu impacte aussi les agents d'utilisateur (UA, *User Agent*) qui sont les "programmes de messagerie ordinaire").

Un UA fait deux choses :

1) Il lit les messages à partir d'une boîte aux lettres et les affiche à l'écran. Cela utilise normalement un protocole comme POP, IMAP ou NFS.
2) Il lit le texte à partir du clavier et le passe au MTA de la boîte aux lettres pour le livrer comme message. Cela utilise normalement le protocole SMTP, c'est à dire le même protocole que celui utilisé entre les MTA.

Lorsque les MTA commencent à mettre en œuvre divers filtres anti-relais comme décrit ci-dessus, un UA sur un hôte d'ordinateur portable PEUT obtenir une réponse comme "Relais refusé" juste parce que il se trouve utiliser des adresses IP au sein d'une gamme inconnue ou qu'elles se résolvent en des FQDN inconnus.

La victime typique de cette réponse "Relais refusé" est un commercial en voyage d'affaires avec son ordinateur portable, ou même un délégué à l'IETF dans l'hôtel où se tient la réunion. Le commercial va probablement téléphoner à son FAI le plus proche et obtenir une adresse IP de ce réservoir téléphonique ; le délégué à l'IETF va utiliser une adresse IP à partir de la pièce des terminaux. Dans les deux cas, leur programme de messagerie d'ordinateur (l'UA ; par exemple, pine, Netscape, Eudora) va essayer d'envoyer les messages via leur MTA de rattachement, par exemple SMTP-SERVER= mail.home.example, mais sauf si mail.home.example a été mis à jour pour accepter cette adresse IP (temporaire) il va répondre "Relais refusé" et refuser.

Pour résoudre ce problème, on pourrait simplement ajouter le réseau IP de la pièce des terminaux ou du réservoir téléphonique à la liste des réseaux acceptés à mail.home.example. Cela ouvre un risque minimal que des envoyeurs de pourriels utilisent cet hôte comme relais de messagerie: Si ils utilisent le même réservoir téléphonique du FAI et qu'ils sont configurés à utiliser mail.home.example au même moment que notre commercial est en voyage, l'envoyeur de pourriels sera autorisé à relayer ses pourriels par mail.home.example. Cependant, ceci est assez improbable et pour autant qu'on ne soit pas ouvert tout le temps à tous les vents et qu'on surveille de près les fichiers de journalisation et qu'on arrête de relayer aussitôt qu'on découvre qu'on est utilisé, cette solution est probablement assez bonne.

Une autre façon est que notre commercial utilise un relais de messagerie fourni par le FAI téléphonique actuel, si ce service existe. Pour ce faire, il doit modifier SMTP-SERVER= dans son UA, ce qui peut ou non être raisonnable.

La façon correcte de traiter cette situation, est cependant de passer par un autre protocole d'envoi de messagerie entre l'UA et le MTA. Bien qu'il n'existe pas d'autre protocole de soumission, un profil de SMTP pour cela, la spécification de "soumission de message", [RFC2476], a été récemment défini.

Ou, on pourrait noter que lorsque le travail d'authentification SMTP, [RFC2554] sera en place, il va permettre à un SMTP authentifié de servir de protocole entre les UA et le MTA de rattachement (on ne se soucie pas ici de savoir si ce DEVRAIT être considéré comme un nouveau protocole ou "le même vieux SMTP").

Cela ajoute un élément à l'algorithme de relais suggéré au paragraphe 2.1 :

\+ Si "authentifié par SMTP", accepter alors de relayer.

3.2. Filtres anti-pourriels personnels

Comme tous les utilisateurs sont individuels, il y a peu d'espoir qu'une action anti-pourriels centralisée convienne à tous – en fait, les gens peuvent invoquer des atteintes à la liberté d'expression, et ils le font, si un ensemble central de règles anti-pourriels est mis en application sans l'approbation des utilisateurs. (On pourrait bien sûr aussi dire que les pourriels n'apportent rien à personne, mais il DOIT appartenir à chaque individu de décider, plutôt que de dépendre d'une décision centrale).

Donc, la seule extension raisonnable est de permettre des filtres personnels anti-pourriels, c'est-à-dire, des filtres anti-pourriels comme ceux décrits plus tôt dans le présent mémoire, mais disponibles et configurables usager par usager. Comme la plupart des usagers n'auront pas une opinion bien définie (sauf ceux qui veulent éviter les pourriels) le système de messagerie DEVRAIT fournir un système par défaut et donner à chaque utilisateur la capacité à outrepasser ou modifier cela. Dans un environnement fondé sur UNIX, on pourrait avoir quelque chose comme :

/etc/mail/rc.spam
~/.spamrc

et des règles sur la façon dont l'un peut interférer avec l'autre.

Tout ceci soulève un assez grand nombre de questions non résolues, par exemple si chaque usager DEVRAIT réellement lui-même décider des codes de retour SMTP (et comment ils DEVRAIENT être décrits pour qu'il en comprenne assez les implications) et comment les systèmes de messagerie existants vont traiter les réponses différentes des divers usagers, en

particulier comment ils vont traiter un mélange de codes 5xx et 4xx :

C MAIL From: <usr@spam.example>
S 250 <usr@spam.example>... envoyeur ok
C RCPT To: <usr@domain.example>
S 250 <usr@domain.example>... receveur ok
C RCPT To: <foo@domain.example>
S 451 <foo@domain.example>... Refusé à cause de la liste des envoyeurs de pourriels
C RCPT To: <bar@domain.example>
S 550 <bar@domain.example>... Refusé à cause de la liste des envoyeurs de pourriels

On peut bien sûr décider de faire soit "250 OK", soit "550 Refusé" sans autre solution de remplacement pour l'utilisateur individuel, mais cela doit aussi être expliqué suffisamment pour qu'un utilisateur ordinaire comprenne les implications du "Refuse 'MAIL From: <.*@spam.example>'" et qu'il puisse éliminer, ou bloquer, les messages qu'il voulait en fait recevoir.

3.3 Authentification SMTP

L'authentification SMTP de la [RFC2554] a déjà été mentionnée comme une méthode pour autoriser le relais de messagerie, mais bien sûr, il y a bien plus que cela. Lorsque cette infrastructure et cette fonctionnalité est en place, les envoyeurs de pourriels auront plus de difficultés à falsifier les adresses et à se cacher.

3.4 Pourriels et NAT

Avec l'augmentation de l'utilisation des traducteurs d'adresse réseau (NAT, *Network Address Translator*) peut venir un besoin accru d'informations supplémentaires dans les fichiers de journalisation. Tant qu'il y a une correspondance univoque entre les adresses à l'intérieur du NAT et les adresses utilisées à l'extérieur, tout va bien, mais si la boîte de NAT traduit aussi les numéros d'accès (pour combiner de nombreux hôtes internes en une seule adresse externe) on va avoir besoin d'enregistrer non seulement les adresses IP des hôtes de pourriels, mais aussi les numéros d'accès. Autrement on ne va pas être capable d'identifier les hôtes individuels à l'intérieur du NAT.

4. Considérations pour la sécurité

L'augmentation semblable à un feu de broussailles des pourriels soulève plusieurs problèmes de sécurité qui, en fait, font courir un risque à l'ensemble de la communauté Internet de la messagerie :

- Les gens PEUVENT échouer à trouver les messages importants dans leurs boîtes aux lettres submergées. Ou, ils PEUVENT les supprimer en la nettoyant.
- Les FAI ont des hôtes de boîtes aux lettres surchargés et des disques pleins. Nettoyer et aider les abonnés exige des quantités de ressources humaines. En fait, les serveurs de messagerie des FAI sont coincés par trop de messages.
- Alors que les disques sont inaccessibles, soit parce qu'ils sont pleins ou à cause de "quotas de messages", des messages importants PEUVENT être retardés ou perdus. Normalement, cela ne va pas se produire sans avertissement, mais si l'hôte envoyeur et l'hôte receveur ont tous deux leurs disques submergés, les messages retournés PEUVENT aussi échouer, c'est-à-dire que le service de la messagerie électronique PEUT devenir moins digne de confiance qu'auparavant.
- Les hôtes utilisés comme relais non autorisés de messagerie sont surchargés. À côté des implications techniques, cela exige aussi des ressources en personnel, pour nettoyer les files d'attentes de messages et prendre soin des utilisateurs externes exaspérés qui ont été inondés de pourriels à travers le relais.
- La lutte contre les envoyeurs de pourriels inclut de bloquer leurs hôtes (ce qui est décrit dans le présent mémoire). Cependant, il y a un grand risque que les hôtes de relais de messagerie puissent être bloqués eux aussi, même si ils sont aussi des victimes. À long terme, cela PEUT causer une détérioration du service de messagerie de l'Internet.
- L'utilisation courante d'adresses "MAIL From:" et "From:" falsifiées fait porter le blâme sur des personnes/hôtes/organisations innocentes. Cela est mauvais pour leur réputation et PEUT affecter les relations d'affaire.

Plusieurs des méthodes décrites dans le présent document augmentent la charge de plusieurs systèmes de soutien du système de messagerie lui-même. Ces systèmes de soutien peuvent être le DNS, le système de journalisation, des bases de données avec les listes des utilisateurs locaux, des mécanismes d'authentification, et autres. La mise en œuvre des méthodes décrites dans le présent document va, à cause de cela, augmenter le risque d'attaque de déni de service contre le système de soutien par l'envoi de pourriels sur un site. Les facilités de journalisation DOIVENT, par exemple, être capables de traiter plus d'enregistrements (qu'arrive t-il lorsque les fichiers de journalisation remplissent le disque ?). Les serveurs du DNS et les mécanismes d'authentification DOIVENT être capables de traiter la charge des recherches supplémentaires, etc.

Les fonctions des systèmes de soutien durant les fortes charges DEVRAIENT être étudiées soigneusement avant la mise en œuvre des méthodes décrites dans le présent document.

Le système de messagerie DEVRAIT être étudié avec attention, par exemple comment il se comporte lorsque un ou plusieurs des systèmes de soutien nécessaires pour une méthode spécifique échouent. Un serveur de messagerie NE DOIT PAS répondre "Échec permanent" (5xx) si il y a un problème temporaire avec un ou plusieurs systèmes de soutien.

5. Remerciements

Le présent mémoire résulte de discussions au sein d'un groupe ad hoc de FAI et universitaires suédois. Sans espérer mentionner chacun on donne simplement ici les noms de domaines : algonet.se, global-ip.net, pi.se, swip.net, telia.net, udac.se; chalmers.se, sunet.se, umu.se, et uu.se.

Nous tenons à remercier de leurs précieux apports et suggestions Andras Salamon, John Myers, Bob Flandrena, Dave Presotto, Dave Kristol, Donald Eastlake, Ned Freed, Keith Moore et Paul Hoffman.

Finalement un grand merci à Harald Alvestrand et Patrik Faltstrom, à la fois de leurs utiles commentaires et de leur soutient et leur guidage à travers les processus de l'IETF.

6. Références

[RFC0821] J. Postel, "Protocole simple de transfert de messagerie", STD 10, août 1982.

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par la* RFC6604)

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC2065] D. Eastlake 3rd, C. Kaufman, "Extensions de sécurité du système de noms de domaines", janvier 1997. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

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

[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.)*

[SENDMAIL] Page d'accueil Sendmail : http://www.sendmail.org

Adresse de l'éditeur

Gunnar Lindberg
Computer Communications Group
Chalmers University of Technology
SE-412 96 Gothenburg,
SWEDEN
téléhone : +46 31 772 5913
fx : +46 31 772 5922
mél : lindberg@cdg.chalmers.se

Déclaration complète de droits de reproduction

Remerciement

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