

**Groupe de travail sur le pourriel
Sous-groupe sur la gestion des technologies
et des réseaux**

**Vue d'ensemble
de la technologie anti-pourriel**

**Services techniques d'homologation
et de télécommunications
Industrie Canada**

mai 2005

Table des matières

Résumé.....	5
Portée	5
Abréviations.....	5
1. Introduction.....	6
2. Vue d'ensemble	7
2.1 Technologies de courriel.....	8
2.1.1 Protocole de transfert de courrier simple et extensions	8
2.1.2 Protocole POP et protocole de messagerie IMAP	9
2.1.3 Protocole MIME, Intimité plutôt bonne (PGP) et protocole SMIME	9
2.1.4 Technologies Web	9
2.2 Catégorisation des pourriels.....	10
2.2.1 Pourriels reçus par courriel	10
2.2.2 Pourriels par messagerie instantanée	11
2.2.3 Pourriels par téléphonie Internet.....	11
2.3 Sources des pourriels	12
2.3.1 Relais ouverts.....	12
2.3.2 Comptes jetables	13
2.3.3 Mandataires.....	13
2.3.4 Ordinateurs hôtes compromis	14
3. Technologies anti-pourriel.....	16
3.1 Filtrage des messages.....	16
3.1.1 Filtres de contenu.....	16
3.1.2 Filtres de hachage	16
3.1.3 Filtres statistiques.....	17
3.2 Listes d'adresses.....	17
3.2.1 Systèmes basés sur le système de nom de domaine.....	17
3.2.2 Listes d'utilisateurs dynamiques	18
3.3 Authentification du serveur client.....	18
3.3.1 Authentification SMTP.....	18
3.3.2 Protocole POP avant le protocole SMTP.....	19
3.3.3 Protocole TLS (Transport Layer Security)	19
3.4 Filtrage et inspection de paquet	20
3.4.1 Filtre egress du protocole SMTP	20
3.4.2 Coupe-feu.....	20
3.4.3 Surveillance du trafic et limitation du nombre de courriels.....	20
4. Nouvelles technologies	22
4.1 Authentification du domaine.....	22
4.1.1 Sender Policy Framework.....	22
4.1.2 Identification de l'expéditeur	23
4.1.3 Domain Keys (clefs de domaine).....	24

4.1.4 Identified Internet Mail	24
4.2 Protocole Internet (IP) version 6	24
4.3 Présence	25
Analyse	25
Conclusion	26

Résumé

Le présent document expose en détail les problèmes ayant trait à la distribution et à la prévention du courriel non sollicité, ou pourriel. Il donne une vue d'ensemble des technologies en place ou nouvelles utilisées pour lutter contre le pourriel. Les méthodes employées pour distribuer le pourriel et échapper aux technologies anti-pourriel y sont également analysées. Le but du présent document consiste à expliquer les méthodes techniques utilisées, afin de faire mieux comprendre les questions qui sont en jeu.

Portée

Le présent document traite des sujets entourant le pollupostage par courriel et les technologies employées pour le prévenir. On y présente les technologies de pointe, mais le document ne devrait pas être jugé exhaustif. Il sera révisé à l'avenir en fonction de l'évolution des technologies anti-pourriel et devrait donc être considéré comme un document en cours d'évolution.

Abréviations

CAN-SPAM	<i>Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003</i>
DNS	Système de nom de domaine
IIM	Courrier Internet identifié
IMAP	Protocole de messagerie IMAP
MAPS	Mail Abuse Prevention System
MARID	Mail transfer agent authorization records in DNS
MIME	Protocole MIME
MTA	Agent de transfert de messages (serveur)
MUA	Agent d'utilisateur (client)
MX	Messageur
POP	Protocole POP
RBL	Real-Time Black Hole List (liste noire en temps réel)
SMTP	Protocole de transfert de courrier simple
SPIM	Pourriel par messagerie instantanée
SRS	Sender Rewriting Scheme
TCP	Protocole de contrôle de transmission
TLS	Transport Layer Security
VoIP	Voix sur IP

1. Introduction

La messagerie électronique s'est avérée l'un des principaux facteurs à l'origine de l'essor d'Internet. La capacité des utilisateurs d'envoyer des messages à des destinataires à l'autre bout du monde à un coût pratiquement nul a beaucoup nui à d'autres méthodes de transmission des messages comme le télécopieur et la poste.

Le faible coût de la transmission de messages a permis à des expéditeurs non sollicités de livrer leurs messages à l'aide du même média. Certains de ces messages non sollicités ont été qualifiés de pourriels par les utilisateurs. Par le passé, le pourriel était simplement considéré comme un désagrément par de nombreux utilisateurs. Toutefois, au cours des dernières années, le volume de ce genre de messages s'est accru. Souvent, le contenu du message est trompeur, frauduleux ou offensant, et il n'est pas facile d'en identifier la source.

La situation actuelle de la messagerie électronique a soulevé des préoccupations chez beaucoup d'utilisateurs, ce qui a donné lieu à l'élaboration de solutions anti-pourriel. Les solutions relèvent de divers domaines, entre autres des domaines technologiques, juridiques et politiques. Le présent document explique les diverses solutions techniques employées pour lutter contre le pourriel dans les courriels et les technologies de messagerie connexes.

2. Vue d'ensemble

La transmission de courriel a relativement peu changé par rapport au modèle original mis au point au début des années 1980. La figure 1 illustre l'échange d'un message général entre un expéditeur et un destinataire. Il existe des variantes qui peuvent modifier l'acheminement des messages, mais l'échange de base demeure identique. Les variantes peuvent inclure le relais de courriel, les passerelles ou mandataires, certaines techniques d'authentification de l'expéditeur, le courriel Web, etc.

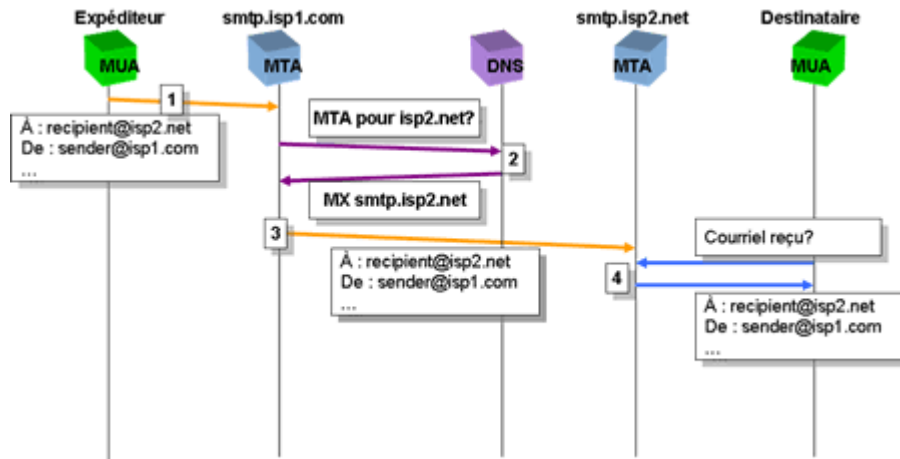


Figure 1 — Séquence type des messages de courriel

1. Un client ou agent d'utilisateur (MUA) élabore d'abord le message à envoyer. Il établit ensuite une connexion SMTP avec son agent de transfert de messages (MTA). Le MUA utilise les commandes SMTP pour identifier l'expéditeur et le destinataire, puis transmet le message au MTA. En pareil cas, le MTA est un serveur de courriel hébergé par le fournisseur de services Internet (FSI) de l'expéditeur.

2. Une fois que le MTA de l'expéditeur a reçu le message, le MTA du destinataire doit être localisé. À l'aide de la partie de l'adresse de courriel du destinataire relative au domaine, une requête est faite au Système de nom de domaine (DNS), demandant l'enregistrement du messenger visant le domaine du destinataire. La liste des serveurs de courriel du destinataire sera alors envoyée.

3. Une fois qu'on connaît l'adresse, une séance SMTP est alors établie, et le message est transmis au MTA du destinataire. Une fois que le message est reçu, il est stocké à des fins de récupération.

4. Le MUA du destinataire utilise le protocole POP ou le protocole de messagerie IMAP pour communiquer avec le serveur et récupérer tout courriel stocké.

2.1 Technologies de courriel

Divers protocoles et technologies permettent d'envoyer et de recevoir du courriel. Les sections qui suivent décrivent brièvement les protocoles les plus courants utilisés pour la messagerie électronique.

2.1.1 Protocole de transfert de courrier simple et extensions

Le Protocole de transfert de courrier simple (SMTP) est celui qui est le plus utilisé pour la transmission de courriel. Au départ, il était utilisé pour échanger des messages textuels entre des nœuds du réseau interne de la Defense Advanced Research Projects Agency du département de la Défense des États-Unis et il a été adopté à grande échelle avec l'essor d'Internet. Le protocole a depuis été perfectionné¹, et des extensions ont été ajoutées².

Le protocole SMTP se voulait simple et solide. Il avait été conçu pour être ouvert, utiliser des commandes interprétables par l'utilisateur et soutenir le relais à travers des réseaux disparates. Ces caractéristiques ont facilité le déploiement à grande échelle du protocole SMTP pour la transmission de courriel, mais ont par ailleurs contribué à une utilisation malveillante du protocole.

En raison de l'acceptation et de l'utilisation du protocole SMTP dans le monde, on croyait qu'il serait très difficile de le remplacer entièrement. Les extensions et les compléments ont amélioré le protocole pendant sa durée de vie, mais certaines de ses lacunes sous-jacentes demeurent.

Pour une transmission solide de messages, le protocole SMTP prévoit un relais par lequel un MTA envoie un message au MTA le plus proche disponible si le MTA récepteur visé n'est pas en ligne ou ne peut être joint. Lorsque le MTA est disponible, le message peut être reçu; dans le cas contraire, le point de relais avisera l'expéditeur que le MTA de destination est inaccessible.

Le relais est nécessaire et constitue une fonction légitime du protocole SMTP. Il est utilisé pour les utilisateurs distants, les services de courriel, le filtrage des pourriels et d'autres fonctions. Pour prévenir l'utilisation malveillante des services de relais, l'accès devrait être limité au moyen de restrictions relatives à l'adresse, de l'authentification SMTP, ou des mécanismes de sécurité du réseau comme la sécurité du protocole Internet ou le protocole TLS (Transport Layer Security).

Les passerelles au niveau de l'application SMTP, également appelées mandataires SMTP, sont utilisées pour transmettre le courriel au-delà des limites du réseau. Souvent, les réseaux d'entreprise utilisent une passerelle SMTP pour traiter le courrier en provenance ou à destination de sources externes, et pour modifier l'information interne sur l'adresse

1. J. Klensin. RFC 2821, *Simple Mail Transfer Protocol*, avril 2001.

2. J. Klensin, N. Freed, M. Rose, E. Stefferud et D. Crocker. RFC 1869, *SMTP Service Extensions*, novembre 1995.

de l'entreprise au moment du passage à travers la passerelle. Similaires à des relais, les mandataires peuvent également être utilisés pour envoyer du pourriel s'ils ne sont pas sécurisés adéquatement.

2.1.2 Protocole POP et protocole de messagerie IMAP

Le protocole POP a été mis au point en vue de récupérer les messages pour des utilisateurs de serveurs de courriel. Sans une méthode de récupération des messages, tous les messages resteraient sur le serveur, et les clients devraient accéder au serveur d'une façon ou d'une autre pour utiliser le courriel ou exploiter leur propre serveur localement. Le protocole POP est devenu largement accepté après la troisième révision (POP3). Un utilisateur POP peut se connecter et recevoir tous les messages, mais le protocole POP n'offre pas un stockage ou une catégorisation adéquate côté-serveur.

Un autre protocole a été conçu pour régler les problèmes de stockage des messages associés au protocole POP. Le protocole de messagerie IMAP permet la synchronisation, l'authentification forte et la gestion des messages sur le serveur (par exemple, stockage par dossier, recherches et statuts des messages).

Les deux protocoles sont encore utilisés aujourd'hui.

2.1.3 Protocole MIME, Intimité plutôt bonne (PGP) et protocole SMIME

Au départ, le texte en clair (texte ASCII de 7 bits) était le seul format possible du contenu des messages SMTP. Pour élargir ce format, le protocole MIME a été élaboré en vue de permettre l'inclusion de photos, de données et de contenu multimédia dans les courriels. Le protocole MIME permettait d'envoyer de nombreux types de contenu, mais ne répondait pas au besoin de confidentialité du courriel.

La confidentialité et l'authenticité sont deux questions qui ont été réglées au moyen de deux méthodes : les extensions PGP et le protocole SMIME. Ces deux normes assurent que le contenu du message ne peut être modifié ou vu par personne d'autre que le destinataire prévu. Pour protéger le message à l'aide de l'une ou l'autre de ces technologies, l'expéditeur et le destinataire doivent pouvoir manipuler le contenu des messages PGP ou SMIME. Les deux clients doivent soutenir la même méthode, soit PGP ou SMIME, contrairement aux serveurs de courriel, qui ne font que transférer le message en fonction des en-têtes, lesquels ne sont pas encodés.

2.1.4 Technologies Web

Les applications Internet de messagerie électronique et de courriel résidant sur le Web seront également analysées dans le présent rapport.

Les services de courriel accessibles sur le Web, ou webmail, sont devenus courants et jouent le rôle d'un client courriel traditionnel. Un utilisateur de webmail a seulement besoin d'un navigateur Web et n'a pas besoin d'un client courriel pour s'occuper des

séances SMTP, POP et IMAP. Les caractéristiques comme la sécurité, la protection antivirus, l'espace d'entreposage et les filtres de pourriel peuvent facilement être mises en place pour les utilisateurs. Souvent, les comptes de webmail sont offerts gratuitement à l'utilisateur et sont subventionnés par les annonces publicitaires.

Tout comme le webmail, les applications côté-serveur peuvent offrir un accès direct à un MTA. La plupart des applications utilisent une interface commune pour que les clients Web communiquent avec l'application. Mentionnons par exemple la possibilité de donner de la rétroaction offerte par un site Web, qui est généralement utilisée par les visiteurs du site pour envoyer des demandes par courriel aux administrateurs du site.

2.2 Catégorisation des pourriels

Le terme général « pourriel » est souvent utilisé pour désigner tout courriel non sollicité et non désiré. Dans le présent rapport, nous mettrons l'accent sur les pourriels reliés au courriel, mais d'autres types comme les pourriels par messagerie instantanée ou les pourriels par téléphonie Internet sont également préoccupants. La présente section renferme une description des divers types de pourriel.

2.2.1 Pourriels reçus par courriel

Le pourriel, pour les besoins de la présente analyse, est considéré comme du courriel de masse non sollicité ou du courriel commercial non sollicité. Le but de ces pourriels est de transmettre des annonces directes au plus grand public possible au coût le moins élevé possible. De nouvelles technologies comme le courriel réduisent le coût de transmission des annonces et ont favorisé la prolifération des pourriels.

Il existe de nombreux coûts associés aux pourriels transmis par courriel, entre autres les coûts d'une faible productivité, la sensibilisation des utilisateurs, les charges de l'infrastructure du réseau et la mise au point et le déploiement de technologies anti-pourriel.

Les propriétés communes qui aident à reconnaître un pourriel sont les suivantes : on ne peut se fier à la source du message ou celle-ci ne peut être authentifiée; les coûts engagés par l'expéditeur sont souvent moins élevés que les coûts totaux engagés par les destinataires; et le contenu du message renferme du matériel offensant, frauduleux ou trompeur non voulu.

Pour transmettre les pourriels par courriel, il faut compiler une liste d'adresses de courriel cibles. Une façon courante d'obtenir des adresses valides de courriel consiste à les recueillir à l'aide d'un logiciel automatisé qui peut parcourir des bases de données publiques et des sites Web à la recherche d'adresses de courriel. Une fois qu'une liste de destinataires est établie, on peut utiliser les outils logiciels pour formuler le contenu et l'en-tête de chaque message. Ces en-têtes et contenus sont adaptés de sorte à cacher la source et à éviter les technologies anti-pourriel comme les filtres. Les messages peuvent ensuite être envoyés à l'aide d'outils automatisés pour répartir la charge de transmission

entre diverses sources (relais, mandataires, etc.). Les sources de pourriels sont abordées en détail à la section 2.3.

Un utilisateur devrait savoir comment les polluposteurs obtiennent les adresses et recueillent les données sur les destinataires de leurs messages. Par exemple, certains pourriels envoyés par courriel peuvent fournir une option de désabonnement en bas du courriel. Un utilisateur devrait cependant faire preuve de prudence lorsqu'il a recours à cette option, car elle peut être utilisée à des fins malveillantes. Le lien peut permettre à un polluposteur d'identifier les destinataires qui ont lu le message. Ceci peut, par conséquent, accroître le volume de pourriels que reçoit un utilisateur. L'option de désabonnement peut également mener à un contenu qui contient une méthode pour exploiter les vulnérabilités du logiciel de navigation du destinataire. Dans certains cas, ces « exploits » sont utilisés pour installer un logiciel pernicieux sur l'ordinateur du destinataire, qui peut ensuite être utilisé pour transmettre des pourriels à d'autres.

2.2.2 Pourriels par messagerie instantanée

La messagerie instantanée peut également servir à envoyer des pourriels, d'où le nom pourriels par messagerie instantanée (SPIM). Les services de messagerie instantanée en direct, comme MSN Messenger, Yahoo! Messenger et Jabber, peuvent également être utilisés pour transmettre des pourriels.

Dans le cas des services de messagerie instantanée en ligne, un annuaire est souvent utilisé pour localiser et identifier les abonnés. Les services d'annuaire peuvent être utilisés pour recueillir les noms d'utilisateur et, par la suite, pour envoyer des messages individuels à chaque abonné. Ce processus peut être automatisé à l'aide d'un logiciel; toutefois, l'expéditeur doit également être un utilisateur du système de messagerie instantanée.

La plupart des systèmes de messagerie instantanée bloquent maintenant, par défaut, les messages provenant d'expéditeurs inconnus, et donnent aux utilisateurs la possibilité de bloquer certains expéditeurs.

2.2.3 Pourriels par téléphonie Internet

Le protocole Voix sur IP (VoIP) pourrait bien réduire le coût d'envoi, par les annonceurs, de communications vocales directes à un public cible. La transmission de pourriels à l'aide de ce protocole et de pourriels synchronisés par téléphonie Internet requiert l'utilisation d'une connexion Internet pour passer les appels ou laisser des messages aux abonnés VoIP.

Les coûts associés aux pourriels transmis par VoIP sont plus élevés que ceux transmis par courriel ou par messagerie instantanée, car les expéditeurs de messages audio engagent des coûts plus élevés pour la bande passante utilisée. La méthode d'envoi des pourriels par téléphonie Internet est similaire à celle employée pour transmettre d'autres pourriels; un logiciel automatisé peut être utilisé pour établir une connexion avec un terminal VoIP.

Une fois qu'une connexion est établie, un message peut être envoyé comme message audio ou être enregistré comme courrier vocal. Contrairement au télémarketing, les pourriels transmis par VoIP peuvent être transmis via les connexions Internet, où il est souvent impossible de vérifier la fiabilité et de retracer les expéditeurs.

L'utilisation d'architectures de réseau sécurisées permet d'empêcher les abonnés de recevoir des appels d'appelants non sécurisés. Toutefois, des méthodes non techniques peuvent être requises pour réduire les pourriels transmis par VoIP.

2.3 Sources des pourriels

La présente section traite des diverses sources de pourriels transmis par courriel et des techniques utilisées pour envoyer des pourriels à partir de ces sources.

2.3.1 Relais ouverts

La capacité d'envoyer du courriel est une caractéristique principale du protocole SMTP. Par le passé, la plupart des relais acceptaient du courrier de n'importe quel hôte, afin d'assurer au mieux la transmission des messages. Lorsqu'un MTA envoie du courrier à partir de n'importe quel hôte, on parle de « relais ouvert ».

Normalement, un MTA est configuré de sorte à envoyer le courrier de clients connus, l'identification reposant généralement sur l'adresse Internet ou sur de l'information d'authentification. Les utilisateurs inconnus d'un MTA reçoivent un avis d'interdiction de la transmission s'ils essaient d'envoyer leur courriel par l'entremise d'un relais sécurisé. Les relais ouverts sont devenus obsolètes depuis les améliorations du protocole SMTP; on juge déplorable le fait de permettre à des clients inconnus d'envoyer du courrier. Les relais ouverts qui sont accessibles au public ont été grandement utilisés de façon malveillante par des expéditeurs anonymes de pourriels. Plusieurs exploitants de réseaux ont interdit les relais ouverts sur leur réseau et disposent de méthodes pour les déceler. Une fois qu'un relais ouvert est localisé, il est généralement inscrit sur une liste pour que les autres serveurs de courriel soient avertis de sa présence. La CAN-SPAM Act of 2003 prévoit des peines si un expéditeur envoie des pourriels via un relais ouvert³. Toutefois, ces peines ne sont utiles que si l'expéditeur n'est pas anonyme.

Pour transmettre des pourriels via un relais ouvert, l'expéditeur doit d'abord trouver un relais ouvert, après quoi il peut l'utiliser pour envoyer des messages à des destinataires cibles. Les expéditeurs utilisent souvent des comptes d'accès commuté ou se connectent via un mandataire pour dissimuler leur identité. Une fois qu'une connexion est établie, le message, y compris la liste des destinataires, est transmis au MTA, et le client peut se déconnecter. Le relais enverra ensuite le message à chaque destinataire, sans aucune autre

3. United States Federal Trade Commission. Public Law 108–187, *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)*, 2003.

intervention du client. Les en-têtes de message consigneront chaque relais supplémentaire par lequel transite le message, ainsi que l'adresse source de l'expéditeur. Cette information peut être utilisée pour informer le fournisseur de services de l'expéditeur des utilisations pernicieuses, ce qui entraîne généralement la fermeture du compte du client.

Un logiciel d'automatisation peut être utilisé pour gérer des listes de relais ouverts, des listes de destinataires et la réussite de la transmission des messages. Ces outils offerts sur le marché ont permis la distribution de courriels de masse non sollicités.

2.3.2 Comptes jetables

L'une des premières façons les plus simples de transmettre des pourriels fut par l'intermédiaire des fournisseurs de services Internet (FSI) qui offraient des comptes d'accès commuté. Un client pouvait ouvrir un compte d'accès commuté avec une carte de crédit. Une fois qu'il obtenait son compte, il pouvait l'utiliser pour envoyer et recevoir du courrier. Ce processus a été utilisé facilement à mauvais escient par les polluposteurs qui ont employé les serveurs de courriel des fournisseurs pour transmettre des pourriels. Une fois qu'il recevait des plaintes, le fournisseur de services Internet pouvait fermer un compte en raison des infractions aux modalités du service. Toutefois, avant même que les plaintes ne soient reçues, le contrevenant avait très probablement déjà fermé son compte.

Pour maximiser l'efficacité des pourriels envoyés par courriel, il faut transmettre un gros volume de messages. Avec le déploiement des technologies à large bande, l'accès commuté a perdu la faveur des polluposteurs.

Similaires aux comptes d'accès commuté, les comptes webmail peuvent également être considérés comme jetables et peuvent être utilisés à des fins frauduleuses par les polluposteurs. En raison des volumes généralement élevés de pourriels requis pour obtenir des résultats positifs, de nombreux comptes sont nécessaires. On peut utiliser des scripts d'automatisation pour ouvrir plusieurs comptes, ou pour envoyer des messages à travers des comptes actifs. Les fournisseurs de services webmail offrent maintenant des moyens de prévenir l'ouverture automatisée de comptes, par exemple en affichant une image de texte interprétable que l'utilisateur doit déchiffrer pour confirmer la validité du compte d'utilisateur.

2.3.3 Mandataires

Un mandataire SMTP peut offrir l'anonymat aux polluposteurs, ce qui est essentiel pour éviter les poursuites. Un mandataire fait office d'intermédiaire entre un client et la ressource désirée. Dans le cas des pourriels envoyés par courriel, un expéditeur envoie un message au mandataire, qui le transmet ensuite au destinataire. Le destinataire du message ne connaît que l'adresse du mandataire, et non pas celle de l'expéditeur.

Les mandataires ont plusieurs utilisations légitimes, par exemple entre des réseaux d'entreprise et des réseaux publics, et sont généralement employés pour stocker temporairement des ressources de réseau ou inspecter le trafic qui emprunte le réseau.

Tout comme les relais ouverts, il existe également des « mandataires ouverts », qui répondent aux demandes au nom de tout client qui se connecte à eux. Les mandataires ouverts peuvent découler d'une mauvaise configuration du logiciel ou, plus vraisemblablement, de l'installation d'un logiciel par un utilisateur malveillant. Les mandataires ouverts peuvent être installés par des utilisateurs malveillants qui exploitent les vulnérabilités des logiciels (cette méthode est examinée plus en détail à la section 2.3.4).

L'une des utilisations les plus évidentes des mandataires ouverts se trouve dans le fait d'envoyer un pourriel tout en cachant l'identité du polluposteur. Pour identifier un polluposteur utilisant un mandataire, l'accès à ce mandataire est souvent requis. Les mandataires peuvent être reliés, ce qui rend encore plus difficile la tâche de ceux qui essaient de retracer la source du pourriel.

Les listes de mandataires ouverts sont tenues à jour et les exploitants de réseaux peuvent les utiliser pour bloquer les pourriels provenant de ces sources⁴.

2.3.4 Ordinateurs hôtes compromis

Pour trouver de nouveaux ordinateurs hôtes en vue de transmettre les pourriels, les polluposteurs ont adopté de nouvelles techniques. Plusieurs de ces techniques ont été employées par des utilisateurs malveillants pendant un certain temps, mais ne sont exploitées que depuis peu par les polluposteurs. Un ordinateur connecté à un réseau, ou ordinateur hôte, est jugé compromis lorsqu'un tiers y installe un logiciel, à l'insu de l'utilisateur, pour le contrôler. Ces hôtes compromis, également appelés zombies, peuvent être utilisés pour lancer des attaques distribuées de déni de service ou pour transmettre des pourriels.

Il existe plusieurs façons de compromettre un ordinateur hôte connecté à un réseau. La façon la plus simple consiste, par la ruse, à amener l'utilisateur à installer un logiciel pernicieux (c'est-à-dire un cheval de Troie). Ces programmes pernicieux se trouvent souvent sur les systèmes de partage de fichiers point à point ou en tant que pièces jointes de courriel.

Il existe une façon plus élaborée de compromettre un ordinateur, c'est d'exploiter la vulnérabilité d'un logiciel qui existe dans un système d'exploitation ou un logiciel d'application. Une fois qu'une vulnérabilité est mise au jour, il faut trouver une façon de l'exploiter, puis une méthode de transmission. Celle-ci peut être simple ou complexe, et prévoir des paquets réseau personnalisés, des pièces jointes de courriel infectées, des téléchargements de fichiers communs point à point infectés, des applications en ligne ou l'une des nombreuses autres méthodes. Pour protéger les ordinateurs hôtes contre ces « exploits », le logiciel doit être mis à niveau (par exemple, à l'aide des corrections provisoires fournies par le fournisseur, des mises à jour de la définition antivirus, d'une

4. <http://opm.blitzed.org>

configuration sécurisée) et les connexions au réseau doivent être protégées (par exemple, à l'aide d'un coupe-feu).

Certains logiciels troyens offrent uniquement un canal de commande qui peut être utilisé comme canal de communication pour installer ultérieurement d'autres programmes pernecieux sans le consentement de l'utilisateur. Pour que quelqu'un contrôle un groupe d'ordinateurs hôtes compromis, il faut établir un canal de communication entre un usager malveillant et les ordinateurs. Souvent, ces canaux peuvent être fermés au moyen d'un coupe-feu et un logiciel anti-virus peut être utilisé pour enlever le logiciel pernecieux. Le virus SoBig, qui a accru le volume de courriels au début de 2003, est un exemple de virus qui a utilisé un mandataire ouvert comme charge.

3. Technologies anti-pourriel

De nombreuses solutions peuvent être utilisées pour combattre les divers types de pourriels envoyés par courriel. Le filtrage des messages d'après leurs propriétés, le blocage des expéditeurs de messages, l'authentification des expéditeurs et l'autorisation des clients sont toutes des méthodes employées pour lutter contre les pourriels.

3.1 Filtrage des messages

En général, la mise en œuvre du filtrage de messages est simple et ne requiert aucune modification aux protocoles de courriel existants. Un filtre bien conçu réduira le nombre de faux positifs (filtrage d'un message qui n'est pas un pourriel) et maximisera l'efficacité du filtre. Les filtres empêchent simplement les pourriels d'entrer dans la corbeille d'arrivée, mais n'arrêtent pas la production de pourriels. La présente section donne un aperçu des types courants de filtres, entre autres des filtres hybrides qui utilisent une combinaison de méthodes de filtration.

3.1.1 Filtres de contenu

Il existe de nombreuses variétés de filtres de contenu, mais comme leur nom l'indique, tous filtrent simplement les messages d'après leur contenu. Les règles du filtre sont normalement définies pour tous les utilisateurs locaux sur un MTA par un administrateur de système. Les règles peuvent être établies pour tout contenu figurant dans l'en-tête, le corps ou les extensions d'un message. Le filtre peut être configuré de sorte à analyser l'en-tête en vue de détecter les champs malformés, à analyser le corps du message pour trouver du contenu relatif au pourriel ou à examiner les extensions de messages comme les pièces jointes.

La plupart des filtres de contenu enregistrent un taux élevé de faux positifs, en particulier quand du courrier légitime renferme un contenu similaire à celui figurant dans la règle du filtre établie. Les règles du filtre de contenu doivent être sans cesse mises à jour pour demeurer efficaces. Les polluposteurs adaptent leurs messages pour éviter les filtres, et ces méthodes d'évitement ont également donné lieu à un contenu formulé bizarrement et à des pourriels renfermant uniquement des images.

3.1.2 Filtres de hachage

Une fois qu'on a observé un nombre suffisant de pourriels, on peut relever les éléments communs, qui peuvent être « hachés » pour donner une valeur unique, laquelle, à son tour, est stockée et utilisée comme règle de filtre. Lorsqu'un filtre de hachage traite un message, les éléments communs sont relevés et hachés. La valeur unique est ensuite utilisée pour déterminer si ces éléments communs ont déjà été classés dans la catégorie des pourriels. Le cas échéant, le message peut être filtré en tant que pourriel. Il est toutefois possible d'éviter les filtres en insérant un contenu insignifiant dans le message pour perturber le traitement des éléments de message communs.

3.1.3 Filtres statistiques

Les filtres statistiques, qui constituent une amélioration par rapport aux filtres de contenu et de hachage, utilisent des règles pour mesurer la fréquence et les caractéristiques des messages de courriel. Le filtre statistique le plus populaire utilisé pour les pourriels est le filtre de type bayésien. Ce dernier calcule la probabilité que des éléments connus se combinent à des éléments supplémentaires pour obtenir un taux de probabilité général qui peut être utilisé en vue de classer un message dans la catégorie des messages légitimes ou des pourriels.

Les filtres de type bayésien produisent un faible pourcentage de faux positifs et leurs règles ne doivent pas être mises à jour par un administrateur⁵. Le filtre s'adapte en surveillant ce que l'utilisateur classe dans la catégorie des pourriels et ajuste les taux de probabilité en conséquence.

Les polluposteurs ont utilisé des méthodes pour éviter les filtres de type bayésien, entre autres l'insertion d'éléments aléatoires de faible probabilité dans leurs messages. L'insertion de ces éléments réduit le taux global de sorte que le message ne sera peut-être pas filtré.

3.2 Listes d'adresses

Les listes d'adresses acceptent ou refusent les messages en fonction de l'adresse de réseau ou du domaine de l'expéditeur. Semblables aux filtres, les listes d'adresses s'avèrent une mesure défensive contre le pourriel, qui ne peut toutefois pas en prévenir la production.

3.2.1 Systèmes basés sur le système de nom de domaine

Les systèmes de listage basés sur le DNS sont devenus un outil essentiel pour identifier les ordinateurs hôtes ou les adresses de réseau qui ont été utilisés pour envoyer des pourriels. Ces systèmes de listage emploient le système DNS pour créer des listes d'adresses de réseau, qui peuvent ensuite être utilisées pour trouver la source des pourriels.

Pour exploiter un système de listage, un exploitant a besoin d'un domaine. Dans ce domaine, les adresses de réseau sont énumérées en tant qu'entrées du domaine en ordre inverse. Par exemple, pour l'adresse 1.2.3.4, l'exploitant doit inscrire l'entrée dans son domaine comme ceci : 4.3.2.1.domaine.net. Les clients qui souhaitent utiliser la liste feront une requête DNS concernant une adresse de réseau précise et l'enverront au DNS de l'exploitant. Si l'ordinateur hôte existe dans les enregistrements DNS, des mesures adéquates seront prises par le client relativement à cette adresse.

5. Kai Wei. *A Naive Bayes Spam Filter*, automne 2003 (www.eecs.berkeley.edu/~kwei/courses/cs281a/cs281a.pdf).

Le premier système à utiliser cette méthode s'est appelé la liste noire en temps réel (RBL), mise à jour par le Mail Abuse Prevention Systems (MAPS)⁶. L'initialisme RBL a depuis été utilisé de façon interchangeable pour d'autres variantes de systèmes de listage DSN. Ces systèmes similaires présentent chacun leurs propres avantages; par exemple, ils n'énumèrent que les mandataires ouverts ou relais ouverts connus.

Les listes DNS doivent être sans cesse mises à jour pour tenir compte des adresses sans cesse changeantes utilisées par les polluposteurs. Ces systèmes peuvent toutefois également bloquer des serveurs de courrier légitimes si les serveurs répondent aux critères des listes. Le processus d'enlèvement des serveurs légitimes devrait être simple et facile à régler.

3.2.2 Listes d'utilisateurs dynamiques

Les listes d'utilisateurs dynamiques identifient les ordinateurs hôtes d'un réseau qui n'ont pas d'adresses de réseau statiques et peuvent changer d'adresse de réseau au cours d'une période. Ces adresses de réseau dynamiques sont utilisées pour les accès commutés et les connexions résidentielles à large bande afin de simplifier le dimensionnement et de permettre une utilisation efficace de l'espace adresse. Les ordinateurs hôtes ayant des adresses dynamiques n'utilisent généralement pas les serveurs de courriel, mais dans de nombreux cas, ils violent les politiques de savoir-vivre en réseau de la plupart des fournisseurs de services.

Les listes d'utilisateurs dynamiques sont tenues à jour par les exploitants de réseau eux-mêmes ou par des organismes tiers. Tout comme d'autres listes d'adresses, elles doivent être tenues à jour de manière rigoureuse pour demeurer efficaces.

3.3 Authentification du serveur client

La présente section traite des diverses méthodes utilisées pour authentifier les clients qui se connectent aux serveurs de courriel ou aux MTA avant que ces clients ne puissent envoyer des courriels.

3.3.1 Authentification SMTP

Dans les réseaux publics, où la méfiance est de rigueur, l'authentification, la confidentialité et l'intégrité sont devenues nécessaires. L'authentification SMTP, extension du protocole du même nom, s'assure que les clients sont en mesure de se brancher à un serveur de courriel. L'authentification en soi n'empêche pas l'usurpation de l'adresse d'un expéditeur ni n'assure la confidentialité ou l'intégrité d'un message. La connexion authentifiée s'établit normalement à un port différent du protocole de contrôle de la transmission (TCP) (c'est-à-dire port TCP 587) plutôt que dans le cadre d'une connexion SMTP ouverte (c'est-à-dire port TCP 25).

6. www.mail-abuse.com

L'extension d'authentification offre deux techniques d'authentification, l'une pour les communications client-serveur (MUA-MTA) et l'autre pour les communications serveur-serveur (MTA-MTA)⁷. Dans le cadre de la première, avant de pouvoir envoyer un courriel, le client est authentifié en entrant un mot de passe associé à un nom-utilisateur donné. Cette méthode peut permettre aux utilisateurs distants de s'authentifier auprès d'un serveur de courriel alors qu'ils se trouvent dans un lieu éloigné.

La deuxième méthode devait uniquement être utilisée dans un environnement fiable et utilisait également la commande d'authentification. Cette commande, utilisée entre les serveurs, indique au MTA récepteur que l'expéditeur a déjà été authentifié.

Il convient également de noter que l'authentification SMTP donne les meilleurs résultats si on utilise simultanément l'extension TLS. En ayant recours à l'authentification et à TLS, on peut sécuriser les séances SMTP.

L'authentification SMTP peut empêcher les polluposteurs d'utiliser sans autorisation les serveurs de courriel. Toutefois, si un polluposteur arrive à compromettre un compte d'utilisateur, il peut ensuite envoyer des messages sans aucune limite. Les spécifications originales prévoyaient l'utilisation de mots de passe faibles; il est donc essentiel d'assurer l'utilisation d'un algorithme de mot de passe fort⁸.

3.3.2 Protocole POP avant le protocole SMTP

Une méthode plus faible que l'authentification SMTP consiste à s'assurer que les clients s'authentifient au préalable auprès de leur protocole de réception de courriel (par exemple, POP). Une fois que le client a été authentifié, le serveur conservera l'adresse de réseau du client et lui permettra de se brancher au serveur SMTP.

3.3.3 Protocole TLS (Transport Layer Security)

Le protocole TLS ou le protocole de sécurisation (SSLv3) peuvent également être utilisés pour assurer une connexion sécurisée entre un client et le serveur. Le protocole TLS peut être observé dans des versions webmail qui utilisent une connexion http sécurisée. Il est également utilisé pour le protocole IMAP afin de sécuriser le transfert de courriel entre le client et le serveur. Le protocole TLS peut également être utilisé avec les versions SMTP pour permettre la transmission sécurisée du courrier par les MTA et les MUA. On appelle également le protocole TLS par le nom de sa commande, STARTTLS, qui est généralement utilisée en même temps que l'authentification SMTP.

7. J. Myers. RFC 2554, *SMTP Service Extension for Authentication*, mars 1999.

8. *Ibid.*

3.4 Filtrage et inspection de paquet

Le filtrage et l'inspection de paquet constituent un très vaste domaine et s'appliquent à de nombreux aspects autres que le pourriel. La présente section porte sur le recours au filtrage et à l'inspection de paquet en ce qui a trait aux pourriels.

3.4.1 Filtre egress du protocole SMTP

Les zombies, ou ordinateurs compromis, constituent la source la plus courante de pourriels. Les zombies peuvent envoyer des pourriels en utilisant la connexion du client à l'insu de ce dernier. Pour empêcher ce trafic, le filtre egress filtre tout le trafic non sollicité provenant d'un client.

Un filtre egress SMTP peut être utilisé pour bloquer les connexions sortantes d'ordinateurs hôtes d'un réseau avec des serveurs de courriel externes. Les filtres egress peuvent être utilisés lorsqu'un ordinateur hôte compromis essaie d'envoyer des pourriels en se branchant aux MTA externes. Si une tentative de connexion est bloquée par un filtre egress, les pourriels ne pourront arriver à destination. Cette méthode réduit la transmission de pourriels sur le réseau et peut aider à bloquer le pourriel avant qu'il n'atteigne les destinataires prévus. Le blocage des connexions peut cependant être controversé et ne devrait pas empêcher les envois légitimes.

3.4.2 Coupe-feu

Les coupe-feu peuvent empêcher l'envoi non autorisé de courrier par des ordinateurs hôtes infectés et l'infection d'ordinateurs hôtes non sécurisés. Un coupe-feu peut permettre ou refuser les connexions entrantes ou sortantes à partir ou à destination d'un ordinateur hôte. Par exemple, la plupart des vers de réseau se propagent en envoyant au hasard des tentatives de connexion à des ordinateurs hôtes. Si un coupe-feu bloque une tentative de connexion entrante, l'ordinateur hôte sera protégé et le ver ne pourra l'infecter. Les coupe-feu peuvent également être utilisés pour autoriser ou refuser les connexions sortantes (par exemple, filtrage egress) et peuvent être appliqués non seulement au SMTP, comme on l'a expliqué dans la section précédente, mais à tout service. Si un ordinateur hôte compromis est utilisé pour transmettre des pourriels, un coupe-feu résidant dans l'ordinateur hôte peut également avertir l'utilisateur de cette activité.

3.4.3 Surveillance du trafic et limitation du nombre de courriels

Au lieu de bloquer les connexions, on peut également surveiller et limiter le volume de trafic dans un réseau. C'est ce qu'on appelle la limitation du nombre de courriels. Les polluposteurs qui compromettent des systèmes envoient souvent de gros volumes de messages, ce qui donne lieu à des courbes de trafic anormales.

La surveillance du trafic peut s'effectuer à n'importe quel point du trajet de transmission d'un message et peut être utilisée pour combattre les pourriels en observant le débit de divers ordinateurs hôtes d'un réseau. Une fois qu'on a déterminé qu'un ordinateur avait

un débit anormal, son propriétaire peut en être avisé et le trafic anormal peut être limité ou bloqué. On réduit à cette fin la largeur de bande disponible et restreint donc la vitesse à laquelle l'ordinateur peut envoyer des messages. Par rapport au blocage, cette technique a pour avantage de permettre l'écoulement du trafic légitime, même si c'est à une vitesse moins élevée.

4. Nouvelles technologies

4.1 Authentification du domaine

Les technologies d'authentification du domaine sont utilisées pour s'assurer que le domaine de l'expéditeur n'est pas usurpé. En raison de l'ouverture du protocole SMTP, un expéditeur peut usurper l'identité d'un autre expéditeur. Cette lacune du protocole est souvent exploitée par les polluposteurs. Pour éviter les poursuites judiciaires ou l'arrêt du service d'un FSI, les polluposteurs doivent rester anonymes. Les améliorations du protocole sont donc nécessaires pour assurer l'authenticité de l'adresse d'un expéditeur. La section qui suit traite de ces améliorations.

Les principaux artisans de ces technologies sont AOL pour Sender Policy Framework (SPF), Microsoft pour Sender ID, Yahoo! pour Domain Keys et Cisco Systems pour Identified Internet Mail (IIM).

4.1.1 Sender Policy Framework

SPF compte une grande base d'utilisateurs et est devenue largement acceptée en tant que méthode courante d'authentification des expéditeurs. Des technologies similaires qui ont rivalisé avec SPF incluent Reverse Mail Exchange (RMX) et le protocole DMP (Designated Mailers Protocol). Toutes ces solutions utilisent le DNS pour authentifier les adresses des expéditeurs. Le but principal de la mise en place d'un plan d'authentification de l'expéditeur consiste à disposer d'une solution unique pour assurer une adoption à l'échelle mondiale.

Le besoin d'une norme unique mondiale est à l'origine de nombreux débats dans le milieu de la conception des technologies. L'Internet Research Task Force formait au départ un groupe de recherche sur les technologies anti-pourriel. Ce groupe a soumis plusieurs spécifications provisoires à l'Internet Engineering Task Force (IETF). Une fois que la nécessité de disposer d'une solution unique est devenue flagrante, le groupe de travail MARID a été formé et chargé d'élaborer la version suivante de SPF. Toutefois, ses membres n'ont pu s'entendre sur une méthode commune. Par conséquent, les activités du groupe de travail MARID ont pris fin le 22 septembre 2004⁹. Tout au long des débats, la version SPF 1 ou SPF Classic a été de mieux en mieux acceptée par les FSI en tant que méthode permettant de valider la source des messages.

SPF authentifie le domaine d'un expéditeur au moyen d'une recherche inverse dans un enregistrement MX dans le DNS. Le processus est similaire à celui qui utilise les enregistrements MX pour localiser le serveur de courriel d'un expéditeur. Un serveur de courrier récepteur utilise le domaine d'un expéditeur et fait une requête à propos de ce domaine. La réponse à cette requête renferme les adresses auxquelles le serveur est autorisé à envoyer le message. Le MTA récepteur utilise l'enregistrement SPF pour vérifier si l'adresse d'envoi est une source de courrier valide. S'il ne peut vérifier

9. www.imc.org/ietf-mxcomp/mail-archive/msg05054.html

l'adresse, on suppose que l'expéditeur a usurpé l'adresse, et le message peut être filtré sur cette base.

On sait que SPF pose problème quand un MTA transmet un courrier au nom d'un destinataire. Le domaine de l'expéditeur original doit passer sans aucune modification, de sorte que la vérification n'échoue pas. SRS (Sender Rewriting Scheme) est l'une des solutions au problème de transmission pour SPF; l'autre est Sender ID.

On craint que les polluposteurs puissent encore avoir recours aux enregistrements SPF pour des domaines pouvant être utilisés pour l'envoi automatique de pourriels. En pareil cas, le pourriel pourra parvenir au destinataire en l'absence d'autres méthodes, mais la source du message demeure connue. Si l'on connaît la source du message, on peut avoir recours à des méthodes comme l'établissement de listes noires, la notification du registraire et les poursuites.

Les domaines jetables peuvent permettre aux polluposteurs d'envoyer des messages authentifiés et d'ensuite simplement enregistrer un nouveau domaine une fois que l'utilisation malveillante a été mise au jour. Ce problème n'a pas encore été réglé, mais une solution partielle peut être l'accréditation du domaine.

4.1.2 Identification de l'expéditeur

Au départ, Microsoft a mis au point le projet Caller ID for E-mail pour authentifier l'expéditeur comme solution de rechange au SPF. Une fois qu'on a compris qu'il fallait une solution globale, les concepteurs de la technologie, avec l'aide du groupe de travail MARID, ont essayé de fusionner les deux projets pour créer une nouvelle spécification provisoire appelée Sender ID.

Le projet Sender ID a une rétrocompatibilité avec SPF. Quand un expéditeur reçoit un message, l'adresse « De » de l'expéditeur est vérifiée en contrôlant un enregistrement DNS pour ce domaine. L'information contenue dans cet enregistrement est utilisée pour s'assurer que le message de l'expéditeur provenait du domaine présumé. Pour régler le problème de transmission relevé dans la version SPF 1 (SPFv1), on a introduit dans la version provisoire l'adresse du responsable prétendu (PRA).

L'algorithme PRA dans la version provisoire Sender ID renfermait les conditions de la licence visant la propriété intellectuelle détenue par Microsoft. Certains projets de source ouverte ne pouvaient accepter les modalités et étaient donc incapables de soutenir cette version. Comme on ne pouvait obtenir un consentement unanime pour le projet Sender ID, les efforts du groupe de travail MARID ont pris fin¹⁰. En novembre 2004, Microsoft a présenté le projet Sender ID lors de l'Email Authentication Summit tenu par la Federal Trade Commission des États-Unis. Le projet a maintenant été approuvé par AOL, qui a appuyé SPF au terme des travaux du groupe de travail MARID.

10. www.imc.org/ietf-mxcomp/mail-archive/msg04673.html

4.1.3 Domain Keys (clefs de domaine)

Domain Keys utilise une méthode différente de Sender ID et SPF pour authentifier les expéditeurs. Pour s'assurer que les utilisateurs peuvent se fier à l'authenticité d'un expéditeur, Domain Keys signe tous les messages au moyen d'une clé cryptographique propre au domaine.

La méthode Domain Keys a recours à un algorithme de clés asymétrique avec des clés publiques et privées. Le MTA expéditeur a besoin d'un MTA activé par clé de domaine, qui utilise une clé privée pour signer le message. Sur réception du message signé, le MTA récepteur examine le domaine de l'expéditeur pour trouver la clé publique de ce domaine. Celle-ci est ensuite utilisée pour vérifier si la signature de l'expéditeur est valide. Si celle-ci s'avère valide, le destinataire peut être certain du domaine de l'expéditeur. Comme pour d'autres protocoles d'authentification du domaine, seuls les MTA doivent prendre en charge la technologie.

4.1.4 Identified Internet Mail

La solution proposée Identified Internet Mail (IIM) est semblable à l'approche Domain Keys, mais ne dépend pas du DNS pour fournir les clés. Elle utilise plutôt un serveur d'enregistrement des clés qui est relié par le DNS. Ce serveur permet l'authentification des ordinateurs hôtes ou de groupes d'ordinateurs hôtes, et non pas simplement du domaine. Le protocole IIM est maintenant rédigé, en même temps que Domain Keys, par le groupe de travail de l'IETF responsable de la rédaction des signatures de courriel.

4.2 Protocole Internet (IP) version 6

L'actuelle version d'IP, IP version 4 (IPv4), limite le nombre d'ordinateurs hôtes adressables qui peuvent être pris en charge par le réseau. Plusieurs de ces adresses ont été attribuées, et on observe une pénurie. Une nouvelle version d'IP, IP version 6 (IPv6), a été conçue et comporte beaucoup plus d'espace adresse. Pour tirer parti de cette taille accrue du réseau et des caractéristiques supplémentaires, IPv6 a commencé à être déployé, notamment dans la région de l'Asie-Pacifique.

Comme IPv6 est généralement déployé, les applications destinées aux serveurs de courriel et les clients devront soutenir IPv6. Le logiciel doit pouvoir interpréter correctement les adresses plus longues qui seront utilisées pour identifier les MTA. La plupart des applications logicielles sont capables de traiter les adresses IPv6; toutefois, certaines devront être mises à niveau. Par ailleurs, les systèmes dont dépend le courriel, comme DNS, les passerelles SMTP et les filtres, devront également pouvoir soutenir IPv6. Les listes d'authentification reposant sur le domaine qui sont utilisées pour bloquer les expéditeurs malveillants devront être modifiées afin d'inclure les expéditeurs adaptés à IPv6. À mesure que les polluposteurs et leurs destinataires opteront pour IPv6, il sera de plus en plus nécessaire de prendre des mesures anti-pourriel adaptées à ce protocole.

4.3 Présence

Le concept de « présence » est utilisé pour fournir des services capables de localiser l'utilisateur pour les applications IM et VoIP. Ces applications ont accès à l'information sur l'emplacement géographique et la situation d'un usager. Cette information doit toutefois être manipulée avec soin. Certains pourriels sans fil exploitent déjà cette information en utilisant des annonces propres à l'endroit, par exemple, dans des aéroports. Si l'information n'est pas bien sécurisée, les technologies IM et VoIP pourraient faire l'objet d'une utilisation pernicieuse de la part des polluposteurs.

Analyse

Vu que le volume de pourriels augmente, il y a lieu d'adopter une approche plus coordonnée pour lutter contre ce fléau. Plusieurs associations industrielles d'exploitants de réseaux ont formulé des recommandations et établi des pratiques exemplaires pour lutter contre les pourriels. L'une des premières à formuler des recommandations a été l'Anti-Spam Technical Alliance, appuyée par des exploitants de gros réseaux et par des fournisseurs de services¹¹. Ses recommandations ont trait à des problèmes connus liés à la limitation des sources conventionnelles de pourriels, comme les relais ouverts, les mandataires et les ordinateurs hôtes compromis. Les recommandations sont jugées très bénéfiques et, si elles sont mises en œuvre, elles augmenteront les coûts pour les expéditeurs de pourriels.

Reste à voir si une seule méthode d'authentification de l'expéditeur pourra être adoptée à l'échelle mondiale et, le cas échéant, si elle permettra de réduire le volume de pourriels transmis par Internet à l'heure actuelle. Comme on l'a mentionné à la section 4.1.2, les membres du groupe de travail MARID de l'IETF n'ont pu s'entendre sur une seule méthode globale. Par conséquent, les discussions se poursuivent concernant diverses méthodes d'authentification des expéditeurs.

D'autres nouvelles technologies, comme les méthodes de signature cryptographique, par exemple IIM, peuvent malgré tout s'avérer une meilleure solution. Toutefois, la méthode d'authentification de l'expéditeur la plus courante et disponible demeure le SPF classique, SPF version 1.

Les pourriels ne disparaîtront qu'une fois que les méthodes de transmission par certains médias ne seront plus rentables. Le coût de transmission de pourriels à l'aide du protocole SMTP augmentera avec les mesures techniques analysées ici. À l'avenir, les polluposteurs opteront pour d'autres technologies plus rentables, comme IM ou VoIP.

11. Anti-Spam Technical Alliance. *Anti-Spam Technical Alliance Technology and Policy Proposal*, juin 2004 (http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf).

Conclusion

L'effort actuel de lutte contre les pourriels a accru les coûts d'envoi des pourriels et donné lieu à des méthodes qui peuvent s'appliquer à d'autres médias. Les technologies anti-pourriel doivent continuer à être mises au point et déployées de manière coordonnée si l'on veut qu'elles soient efficaces. Les nouvelles technologies ont aidé à supprimer l'anonymat des pourriels et peuvent être appliquées à des médias autres que le courriel. Ces technologies, si elles sont utilisées adéquatement, devraient également bénéficier à d'autres mesures anti-pourriel, comme les poursuites.

Même avec l'utilisation de technologies anti-pourriel de pointe, un ordinateur non sécurisé peut facilement être utilisé pour échapper à plusieurs de ces mesures. Le problème doit être réglé au moyen d'une éducation et d'une sensibilisation accrues des utilisateurs courants. Pour réduire le fardeau imposé aux utilisateurs, les solutions technologiques doivent être aussi claires que possible.

Les descriptions des technologies anti-pourriel présentées dans le document visent à donner une vue d'ensemble des technologies actuelles. Les nouveaux problèmes qui se poseront seront abordés dans les révisions subséquentes du présent document en cours d'évolution.

Ouvrages de référence

Anti-Spam Technical Alliance. *Anti-Spam Technical Alliance Technology and Policy Proposal*, juin 2004 (http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf).

J. Klensin. RFC 2821, *Simple Mail Transfer Protocol*, avril 2001.

J. Klensin, N. Freed, M. Rose, E. Stefferud et D. Crocker. RFC 1869, *SMTP Service Extensions*, novembre 1995.

J. Lyon. *Purported Responsible Address in E-Mail Messages*, août 2004 (<http://draft-ietf-marid-pra-00.txt>).

J. Myers. RFC 2554, *SMTP Service Extension for Authentication*, mars 1999.

P. Resnick. RFC 2822, *Internet Message Format*, avril 2001.

United States Federal Trade Commission. Public Law 108–187, *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)*, 2003.

Kai Wei. *A Naive Bayes Spam Filter*, automne 2003 (www.eecs.berkeley.edu/~kwei/courses/cs281a/cs281a.pdf).

Vue d'ensemble de la technologie anti-pourriel