L'impact de la lutte contre le SPAM et les virus sur les architectures de messagerie

Serge Aumont
Comité Réseau des Universités (CRU) Rennes
Serge.Aumont@cru.fr

Claude Gross
Unité Réseaux du CNRS (UREC) Grenoble
Claude.Gross@urec.cnrs.fr

Résumé

L'évolution du phénomène du spam dans son ampleur et dans sa nature ne nous permet plus aujourd'hui de nous contenter de le supporter simplement comme une gêne. Les buts poursuivis par certains spammeurs font courir un risque sérieux à nos systèmes d'informations. Cet article fait le point sur les méthodes techniques de lutte disponibles aujourd'hui en essayant de dégager une typologie. Il propose une approche pour leur intégration dans une architecture de messagerie dans le but de contrer le plus efficacement possible cette menace.

L'article distingue les flux entrant et sortant du domaine. Il explique pourquoi le traitement anti-spam/anti-virus du flux sortant ne doit pas être négligé. Il distingue les techniques binaires qui aboutissent à un rejet ou non des messages de celles qui donnent un résultat insuffisant pour prendre le risque d'un rejet mais, qui corrélées entres elles, permettent cette prise de décision. Un accent particulier est porté sur les nouvelles techniques d'authentification ; SPF (vérification de la provenance des messages) et de DKIM (signature cryptographique) parce que leur impact sur l'architecture de messagerie est particulièrement importante.

1 Introduction

Les raisons d'être du spam trouvent leur origine dans :

- le coût négligeable de l'envoi d'un message et le faible taux de retour nécessaire à sa rentabilité.
- Les faiblesses du protocole SMTP, qui permettent en particulier de falsifier facilement l'adresse d'expédition d'un message (le *spoofing*).
- L'existence de relais de messagerie non sécurisés et de PC infectés par des programmes hostiles qui ont facilité une croissance très forte de ce phénomène.

Les premières conséquences du spam sont évidentes : pour les prestataires de services, le coût de réception et de stockage n'est pas négligeable. Pour les usagers, la perte de temps et d'énergie provoquée par l'encombrement de leur boîte à lettres, le risque de perdre des messages importants noyés dans le flot de spams, le risque d'être victime d'une escroquerie et celui d'apparaître comme l'auteur d'un spam particulièrement indigne sont intolérables.

Mais alors que le spam pouvait être autrefois considéré comme simplement un phénomène dérangeant, il présente également de nos jours des menaces au niveau de la sécurité des systèmes d'information. En effet, on assiste actuellement à une collusion entre les spammeurs et les hackers, les premiers se servant des techniques des seconds pour l'envoi de spams, et les seconds utilisant celles des premiers pour la propagation de leurs virus.

De ce fait les traitements anti-spam et anti-virus sur les serveurs de messagerie doivent nécessairement être vus de façon globale et non pas dissociée.

De plus, le phénomène du spam a évolué vers des pratiques qui relèvent de plus en plus du domaine de l'escroquerie et ceci à un niveau professionnel.

Parmi les menaces les plus sérieuses apparues ces dernières années, on peut citer :

- Le *phishing* [1] qui consiste à émettre du spam à destination d'un grand nombre de personnes dans le but de les inciter à se connecter à des sites imitant parfaitement le portail d'organismes comme des banques afin de récupérer des informations confidentielles (numéro de carte bancaire, codes d'accès, …).
- Les *botnets* [2] ou « ordinateurs zombies » qui sont constitués de PC infectés par un virus informatique ou par chevaux de Troie et contrôlés à distance. Les buts poursuivis peuvent être variés, en particulier la diffusion de spams en grande quantité. Ceci illustre bien le fait que la lutte contre le spam ne consiste pas seulement à éviter d'en recevoir mais aussi de ne pas en émettre, même à son insu.

L'impossibilité pratique de réprimer les abus achève de faire de cette question un enjeu majeur de la sécurité de nos réseaux.

2 Les contraintes de la lutte contre le spam

La lutte contre le spam peut prendre différentes formes, en particulier juridiques ou techniques. Nous ne nous intéresserons ici qu'aux réponses techniques.

La messagerie électronique est l'un des services les plus utilisés sur Internet. Ses utilisateurs sont habitués à une certaine qualité de service qui peut se décrire ainsi :

- Disponibilité du service
- L'envoi d'un message sera reçu par son destinataire dans un délai raisonnable, le plus souvent instantanément (par exemple, il est parfois bien pratique d'utiliser des échanges de messages lors d'une conversation téléphonique)
- Pas de perte de messages
- Facilité d'accès à sa messagerie, qui est le premier service Internet demandé par les utilisateurs nomades

La lutte contre le spam doit affecter le moins possible cette qualité de service, en particulier :

- Bien mesurer l'impact d'un traitement anti-spam en terme de ressources serveurs. Mal évalué il peut parfois entraîner des problèmes pires que le mal qu'il est censé combattre. Un traitement trop coûteux en ressources pour un serveur de messagerie peut, en cas d'augmentation du nombre de messages reçus, entraîner le blocage du service de messagerie.
- Certains traitements aboutiront à un rejet pur et simple des messages incriminés alors que d'autres fourniront simplement une probabilité plus ou moins importante qu'un message est un spam. Dans ce derniers cas, et pour éviter au maximum les faux positifs (et donc éventuellement une perte du message), le message sera marqué (par une modification d'entête) avant d'être acheminé à son destinataire, charge à lui de confirmer ou non le classement en spam. En cas de critères non discriminatoires, c'est à l'utilisateur d'avoir le dernier mot.

Enfin, la lutte contre le spam doit s'inscrire dans la législation en vigueur sur la messagerie électronique, en particulier en ce qui concerne la confidentialité du courrier.

3 Les armes disponibles

Toutes les méthodes techniques utilisables contre le spam, aussi efficaces soient-elles, resteront limitées sans la collaboration active des utilisateurs pour lesquels elles seront mises en place. Une formation de ces derniers, mettant l'accent sur les bonnes pratiques liées à l'usage de la messagerie, est donc absolument nécessaire, ainsi qu'une information sur les outils qui sont mis en place.

Les outils disponibles, non forcément spécifiques, pour lutter contre le spam sont de natures variées et peuvent être classés de la manière suivante :

- Identification de l'émetteur du message soit par signature électronique du message (S/MIME) soit par authentification sur le serveur de messagerie (SMTP/AUTH).
- Protocoles spécifiques visant en général à vérifier la provenance du message (SPF, Caller-id) ou leur authenticité (DKIM, Domain Keys, IIM ...)
- Analyse comportementale consistant à exploiter certains comportements caractéristiques des messages de spams : non respect des RFCs, cadence des messages reçus…
- Filtrage par signature pour détecter la présence de virus, par analyse du contenu des messages, par analyse statistiques (classification bayesienne), par utilisation de bases de données de sources de spams (blacklists) ou par utilisation de bases de données de messages de spams.

Ces techniques peuvent être

- Curatives : refus du message avec ou sans notification à l'expéditeur
- Préventives : marquage simple du courrier pour indiquer qu'il peut s'agir d'un spam.

Les techniques curatives correspondent à des méthodes permettant une prendre une décision déterminante quant à l'acceptation du message traité. Les spams détectés ainsi sont purement et simplement rejetés sans avertissement du destinataire et le plus souvent non plus de l'émetteur. De telles techniques, pour le moment très peu nombreuses, sont de type comportemental comme le greylisting ou la conformité aux RFCs, ou par analyse des entêtes, comme par exemple le test de reverse DNS. Le choix de ces méthodes et la manière de les utiliser doivent être bien évalués avant leur mise en place.

Les techniques préventives, au contraire, aboutiront dans tous les cas à l'acheminement du message traité vers son destinataire. Ce type de filtrage se contente de marquer ou non les messages qu'il traite, indiquant ainsi une probabilité plus ou moins forte qu'il s'agit d'un spam. Pour cela un ensemble de tests est appliqué en utilisant un système de pondération. Au-delà d'un certain seuil, le message est marqué comme spam. Le marquage, qui peut être une modification du sujet du message ou l'ajout d'une entête particulière dans le message, pourra alors servir pour le tri des messages par les utilisateurs soit manuellement soit automatiquement.

Toutes ces méthodes peuvent être utilisées seules ou combinées.

Les logiciels de lutte contre le spam intègrent souvent plusieurs de ces techniques, comme par exemple *J-chkmail* [3] (analyse comportementale, analyse de contenu, listes noires) ou *Spamassassin* [4] (analyse de contenu, listes noires, analyse bayesienne).

Quelques unes de ces méthodes sont décrites succinctement ci-dessous.

3.1 SMTP/Auth et SMTPS

Ces deux méthodes permettent l'identification de l'émetteur d'un message au niveau des serveurs de messagerie

- SMTP/AUTH [5] : utilisation d'un login/mot de passe (l'emploi de TLS est alors fortement recommandé pour assurer le chiffrement du mot de passe)
- SMTPS [6] : utilisation du protocole TLS [7] et d'un certificat X509 pour le client de messagerie.

Elles peuvent être mises en place pour permettre l'utilisation du serveur de messagerie d'un site pour l'émission de messages à partir de l'extérieur de ce site (utilisateurs nomades par exemple).

3.2 Les antivirus

Comme nous l'avons vu ci-dessus, la lutte contre le spam ne peut être dissociée de la lutte contre les virus. Les anti-virus sur les serveurs de messagerie et sur les postes utilisateurs doivent donc être cités dans ce cadre.

3.3 Le greylisting

Le greylisting [8] consiste, lors de la réception d'un message, à renvoyer un code d'erreur temporaire indiquant au serveur de messagerie émetteur qu'il doit réémettre le message après un certain délai. Si le message est réémis correctement, il sera accepté et tout message ultérieur présentant les mêmes caractéristiques (adresse de l'expéditeur, adresse du destinataire, adresse du serveur de messagerie émetteur) sera accepté sans condition pendant un certain temps.

Bien configurée, cette technique présente l'avantage d'être pratiquement transparente pour les utilisateurs et de ne produire pratiquement aucun faux positif.

Malgré quelques problèmes liés à certains serveurs de messagerie gérant mal les codes d'erreurs temporaires, cette méthode est très efficace et réduit de façon spectaculaire le nombre de spams acceptés sur un serveur. En effet, bon nombre de virus et de botnets disposent de leur propre moteur SMTP. Ces moteurs rudimentaires ne font pas de réémission en cas d'échec. Cette source majeure de spams est donc contrée par le greylisting.

On peut hélas supposer que dans un avenir proche les outils des spammeurs seront adaptés pour contourner cette défense.

3.4 Listes noires et listes blanches

Les listes noires ou blacklists sont des listes de sources connues de spams :

- Adresses connues de spammeurs
- Fournisseurs d'accès spammeurs
- Relais de messagerie ouverts

Ces listes peuvent être gérées localement sur un site ou accessibles sur un serveur distant. Dans ce dernier cas, leur utilisation peut être gratuite ou payante, et le principal problème est la qualité de leur gestion.

A l'inverse, les listes blanches sont des listes de partenaires de confiance destinées à éviter les faux positifs ou certains traitements du filtrage.

3.5 Bases de spams

Il s'agit de bases de données, gérées de façon collaborative, contenant l'empreinte de messages de spams connus. L'empreinte de chaque message reçu est comparée au contenu de cette base. *Razor* [9] et *DCC* [10] sont deux exemples de telles bases.

3.6 Analyse du contenu des messages

Cette technique consiste à procéder, par un ensemble de tests, à une analyse lexicographique et syntaxique du corps et des entêtes des messages afin d'essayer d'y retrouver certaines caractéristiques connues des messages de spams :

- Mots clés et leurs dérivés (*sex*, *viagra*, …)
- Expressions régulières pour retrouver des tournures de phrases
- Liste d'URLs interdits
- Utilisation particulière de format ou de code dans le corps (HTML, code javascript, images, …)
- Valeurs d'entêtes de messages suspectes

Le résultat de chacun des tests effectués augmentera ou non un score global qui indiquera une probabilité plus ou moins forte que le message traité est un spam. Au-delà d'une certaine valeur, le message sera marqué.

La panoplie de tests est figée à un instant *t*. De ce fait les logiciels utilisant ce genre de traitement doivent être constamment améliorés car les spammeurs utilisent des techniques de plus en plus évoluées pour les contourner.

3.7 Analyse bayesienne

Cette méthode d'analyse statistique se base également sur le contenu entier des messages, aussi bien les entêtes que le

corps du message. Elle permet d'associer des probabilités aux mots contenus dans les courriers. En fonction du pointage obtenu, la probabilité qu'il s'agisse vraiment de spam augmente ou diminue.

Pour être réellement efficace, cette méthode requiert une phase d'apprentissage par l'alimentation d'une base en indiquant les messages qui sont des spams et ceux qui ne le sont pas (ham).

Cette méthode est maintenant implémentée comme fonctionnalité dans beaucoup de logiciels de courrier électronique.

Elle peut être également utilisée de façon globale sur un serveur de messagerie avec des produits comme *Spamassassin* [4] ou *Bogofilter* [11]. Dans ce cas se pose alors le problème de l'apprentissage et il est nécessaire de fournir aux utilisateurs une procédure pour alimenter correctement la base de connaissance. Cette condition levée, l'analyse bayesienne est préférable au niveau d'un site car plus le volume de messages traités est élevé, plus le filtrage sera performant. Ceci est vrai même si les domaines d'activités des utilisateurs sont différents, car :

- un vrai message de spam l'est pour tout le monde
- les messages considérés comme spam par telle catégorie de personnes et non par une autre sont peu nombreux.

4 Les techniques d'authentification

Constatant que SMTP permet le plus simplement du monde d'usurper une adresse messagerie fictive ou réelle, la communauté des experts motivés par la lutte contre le spam recherche un accord sur de nouvelles techniques d'authentification des messages.

SPF (Sender Policy Framework) [12] et DKIM (*Domain Keys Indentified Mail*) [13] sont les deux tentatives les plus représentatives des orientations choisies.

Les détracteurs de ces technologies objectent souvent que rien n'empêche les spammeurs d'utiliser ces standards. Certains avancent même que la part des messages utilisant correctement ces techniques serait plus élevée dans le spam que dans le ham. L'authentification serait donc une arme vaine dans la guerre contre le spam. Il convient cependant de ne pas oublier que l'usurpation d'adresses email est en elle-même une plaie de la messagerie ; elle affecte grandement la confiance que nous pouvons placer dans le service. Les efforts pour déployer S/MIME et PGP attestent de cette difficulté. Par ailleurs, l'authentification des messages, même si elle ne constitue pas en elle-même une défense, est un préalable aux sanctions que peuvent prononcer des tribunaux au bon fonctionnement des services dit de « réputation » (blacklist, whitelist et les techniques analogues avec un facteur de pondération).

Nous voulons encourager notre communauté à mettre en œuvre SPF dès maintenant et DKIM dès que le RFC et les implémentations seront stabilisés. Nous discuterons les conditions de l'architecture du service de messagerie compatible avec le déploiement de ces deux nouveaux services.

4.1 Authentifier le parcours des messages : SPF

SPF: Sender Policy Framework [12] est parfois appelé « S*ender Permitted From* ». Cette appellation correspond assez bien au principe sur lequel est basé SPF : l'enregistrement dans le DNS d'informations permettant de vérifier si une machine donnée est autorisée à émettre un message pour un domaine donné. La vérification porte sur le `Return-path.` Cette technique n'est pas infaillible mais si elle était généralisée, elle permettrait de repérer certaines usurpations d'adresse, en particulier celles utilisées par une grande partie des spammeurs.

L'hypothèse qui sous-tend SPF est que le *postmaster* d'un domaine peut contrôler via son DNS la liste des MTA autorisés à émettre des messages pour le domaine et que toute autre machine le faisant correspondrait à un cas d'usurpation. L'enregistrement SPF est une sorte de « reverse MX » utilisé par le MTA recevant le message.

En outre, l'enregistrement DNS SPF (un enregistrement de type texte qui n'impose donc aucune modification des serveurs de noms existants) indique comment l'on doit traiter les messages non conformes à la politique de routage exprimée pour le domaine concerné.

En dehors du statut « *pass* » (succès) ou « *fail* » (échec), le test SPF peut aussi retourner les valeurs « *softfail* » (message suspect) et « *neutral* » (résultat non significatif) ne conduisant pas directement au rejet du message.

L'utilisation de SPF est largement décrite sur le site du groupe de travail anti-spam WG-antispam [14].

4.1.1 SPF et le forwarding

Le *forwarding* est une technique de réémission de messages qui, par opposition au « *remailing* » ne réécrit pas l'enveloppe du message. Ainsi, quand un message est retransmis par le MTA destination vers une nouvelle adresse, le Return-Path : du message est inchangé alors que le MTA émetteur n'est plus le MTA d'origine. Le *forwarding* est largement utilisé, c'est un service apprécié des utilisateurs qui changent d'ISP et font suivre leurs messages vers leur nouvelle adresse.

Pour palier à cette limitation, plusieurs propositions ont été faites. SRS (Sender Rewriting Scheme), est une technique de réécriture du Mail From : qui n'affecte pas le test SPF. Avec SRS, si le MUA de « bob@forwarder.org » redirige un message de « ann@orig.org » vers une autre adresse, le « MAIL FROM : » de la nouvelle session SMTP ressemble à « srs0+yf09=Cw=orig.org=ann@forwarder.org »

Responsible Submitter est une alternative qui étend l'élément de protocole SMTP EHLO. Pour le même exemple le « MAIL FROM : » devient :

```
MAIL FROM:<ann@orig.org> SIZE=1000
SUBMITTER=<bob@forwarder.org>
```

SPF ne fait donc pas l'unanimité principalement parce qu'il est douteux que SRS ou « responsible submitter », en théorie préalable indispensable, puissent être un jour déployés. Les détracteurs de SPF soulignent que SPF ne devrait pas être utilisé avant que l'une ou l'autre de ces propositions visant à régler le cas du forwarding ne soit déployée à l'échelle de l'internet [15].

4.1.2 Utilisation de SPF en lieu et place d'une whitelist

Bien que les arguments contre SPF soient incontestables, cette technique ne doit pas être abandonnée si facilement. L'utilisation du statut « *neutral* » permet de lever les contre indications à SPF. Certes, dans ce cas, SPF utilisé seul ne permet plus de rejeter des messages ni même de réellement de détecter les usurpations d'adresse, mais le statut SPF peut devenir un critère de plus dans une stratégie anti-spam. Dans le cadre de l'utilisation du greylisting, il peut être beaucoup plus facile d'utiliser le statut SPF *pass* comme critère d'exception plutôt que de gérer une whitelist. Ainsi, nous pourrions publier une liste des domaines de notre communauté pour lesquels un statut SPF pass permettrait de ne pas être pénalisé par greylist. Cette technique déjà employée laisse à chacun la responsabilité de publier dans le DNS la liste de ses serveurs sortants et nous dispense d'une gestion centralisée d'une liste de plusieurs milliers de hosts.

4.2 Authentifier les messages : DKIM

DKIM Domain Keys Identified Mail [13] est décrit dans l'article « *Signature des message : une réponse contre le spam ? »* de François Morris [16]. En voici cependant les grandes lignes. Dans ce cas l'objectif n'est plus d'identifier la provenance des messages mais d'authentifier les messages eux-mêmes. Le message (mis sous forme canonique) est signé en utilisant un algorithme d'empreinte (SHA1) et un algorithme de chiffrement asymétrique (RSA) selon les mêmes grands principes que pour les signatures S/MIME ou PGP. La signature est placée dans les entêtes du message (à noter que certaines entêtes sont incluses dans la forme canonique utilisée pour calculer l'empreinte du message ; elles ne sont donc pas falsifiables).

DKIM présenté durant l'été 2005 est une synthèse de précédentes propositions (DK et IIM) ; ce draft est peut être appelé à un large succès. En effet, les auteurs de DKIM proposent une solution d'authentification qui ne s'encombre pas de tous les concepts sophistiqués de S/MIME et des PKI, mais qui répond à l'absence totale d'authentification de SMTP de façon très sérieuse. Deux difficultés majeures freinant le déploiement de S/MIME sont contournées dans DKIM :

- DKIM n'a pas besoin de PKI. Les clés publiques sont diffusées via le DNS dont l'organisation constitue de fait l'espace de confiance de l'internet. La confiance que l'on peut accorder à une signature DKIM est donc celle que chaque utilisateur d'internet accorde au DNS et à son système de délégation hiérarchique.
- DKIM permet d'appliquer la signature au niveau d'un MTA et nous dispense donc de distribuer des clefs privées aux utilisateurs. La clé privée de signature peut être spécifique à chaque utilisateur ou partagée par tout ou partie des utilisateurs d'un domaine. Dans les deux cas, elle peut être stockée si on le souhaite, sur un serveur.

4.2.1 Sender Signing Policy

Ce RFC complémentaire de DKIM, permet de décrire la politique de signature pour le domaine ou pour une personne. Il permet de préciser que l'absence de signature peut être considérée comme normale ou au contraire que tous les messages de cette entité doivent être signés, directement ou via un tiers (par exemple une liste de diffusion ou un sous-traitant).

4.3 S/MIME

Utilisant le format MIME, S/MIME permet d'ajouter différents services de sécurité à la messagerie électronique: confidentialité, authentification, intégrité et non répudiation des messages. Dans le cadre de la lutte contre le spam, cette technologie permet donc en particulier d'authentifier l'émetteur d'un message. Mais elle implique l'utilisation de certificats électroniques X.509, la mise en place d'Infrastructures de Gestion de Clés (IGC) et de politiques de certification permettant la confiance entre ces IGCs.

La sécurité visée par S/MIME est plus ambitieuse que celle apportée par DKIM, mais la faiblesse des déploiements limite son utilisation contre le spam. Cependant, le fait qu'un message soit signé peut servir de critère discriminant dans le filtrage anti-spam.

5 Typologies des architectures

Le service de messagerie peut être mis en œuvre avec une seule machine et à la limite un seul programme serveur ; cette situation est de plus en plus rare. Examinons les différents composants du service de messagerie :

1. Le service de réception des messages entrants dans le domaine : le MX ;
2. le service de relais interne (Internal Relay, IR) ;
3. le service de remise des messages en boîte aux lettres (Mail Delivery Agent, MDA) ;

4. le serveur de consultation (serveurs IMAP ou POP)
5. l'interface utilisateur MUA ;
6. le Mail Submission Agent ou MSA chargé de la prise en charge de messages émis par les utilisateurs locaux ;
7. Le service de routage des messages sortants du domaine ;
8. Service de filtrage (anti-virus, anti-spam marquage bayesien) ;

Seuls quelques très gros domaines séparent toutes ces différentes fonctions sur des serveurs différents. Cependant, même lorsque l'ensemble de ces services partage un petit nombre de machines, il peut être intéressant de concevoir chaque fonction comme pouvant devenir autonome.

6 Place des méthodes de filtrage dans l'architecture

Un filtrage anti-spam doit répondre à plusieurs contraintes parmi lesquelles : être le plus performant possible dans la détection des spams, impacter le moins possible les usages de la messagerie électronique et être facilement adaptable.

Pour cela, il est nécessaire d'intégrer les différents outils utilisés dans les composants les mieux adaptés de l'architecture de messagerie d'un site. Cette intégration devra tenir compte de différents paramètres : taille du site, volume du trafic de messagerie, puissance des serveurs, etc. En fonction de la situation, les composants pourront être distribués sur différents serveurs ou non.

La figure ci-dessus illustre les différents composants d'une l'architecture de messagerie pouvant jouer un rôle dans le filtrage anti-spam.

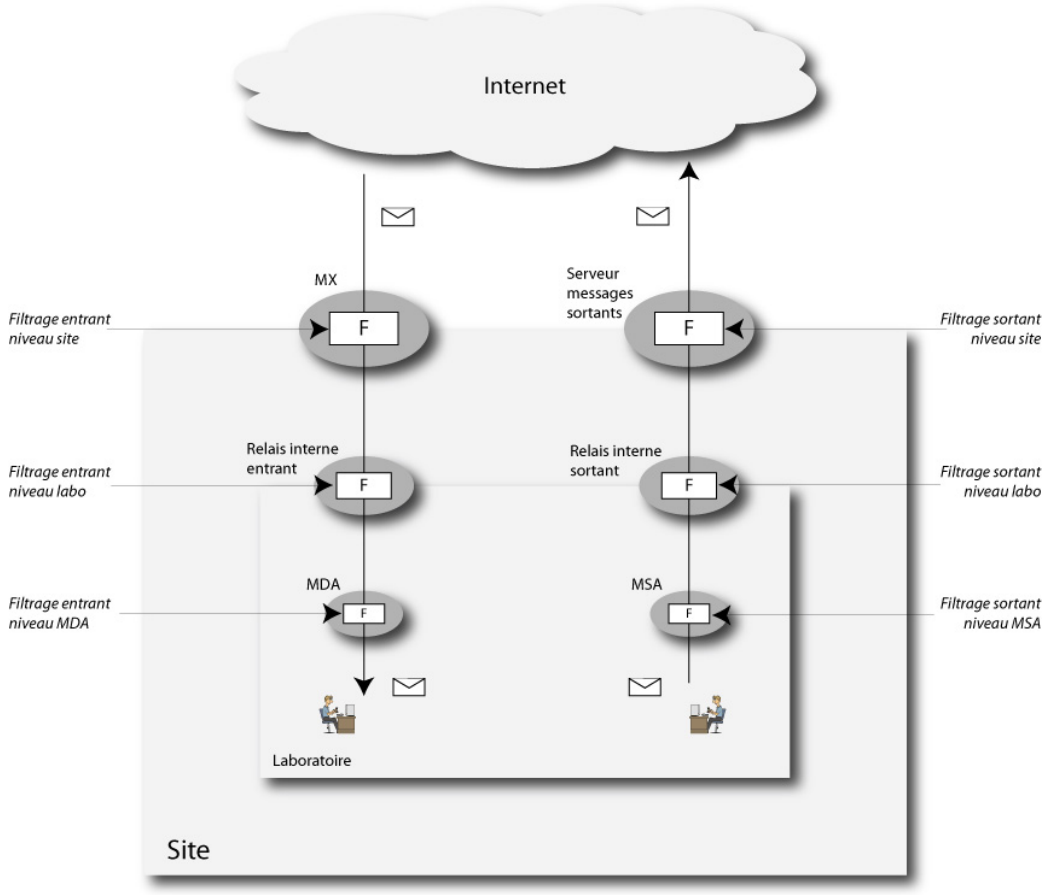

Figure 1

6.1 Les MX

Il importe de bien dimensionner les MX sur lesquels une charge croissante repose. En effet de nombreux arguments poussent à y concentrer les fonctions anti-spam et anti-virus.

1. Il est facile de contrôler ce service en filtrant le protocole SMTP sur les routeurs et en déclarant les MX dans le DNS. Cette clarté technique souligne la responsabilité administrative de la messagerie qui en général est confiée au CRI. Bien entendu, elle expose ce service informatique à de vives critiques en cas de défaillance…
2. Cette centralisation favorise la traçabilité des échanges.
3. Le *greylisting* est obligatoirement placé sur ce premier élément du service de messagerie car dès lors que le message serait accepté et relayé vers un autre serveur, il ne serait bien entendu plus possible d'y recourir.
4. En appliquant les filtres anti-virus dès cette étape on garantit une administration centralisée de cette fonction de sécurité essentielle. Le filtrage peut être fait sur la machine locale ou via un serveur de filtrage, par exemple en utilisant l'interface *milter* de sendmail. Il apparaît cependant que le traitement anti-virus étant lourd, cette organisation risque de mettre à mal la disponibilité du service MX lors de crises (*mail bombing*, nouveaux virus très contagieux, etc).
5. Les filtrages anti-spam conduisant à des rejets purs et simples des messages peuvent avantageusement être placés sur les machines MX. En effet, dans ce cas, le rejet du message intervenant durant la session SMTP entrante, le serveur envoie un code d'erreur et n'a donc pas à générer un message de rejet. Cette situation est confortable car nous savons que très souvent il ne faut pas générer de rapport de non-remise (*bounce*). Celui-ci, adressé à une personne dont l'adresse aurait été usurpée, contribuerait à la pollution de la messagerie. Cependant, rejeter un message sans code d'erreur ni *bounce* est contraire aux RFCs et peut conduire à la perte pure et simple d'un message licite. L'envoi d'un code d'erreur en session est donc la solution idéale car elle dispense le MTA de choisir de générer ou pas un rapport d'erreur.
6. Le round robin DNS permet de déclarer plusieurs machines MX et de faire de la répartition de charge des différents MX. On peut donc augmenter la puissance disponible indéfiniment ou presque. Dans ce cas il est impératif que la solution retenue pour le *greylisting* permette le partage des données conservées en liste grise[1]. Des produits comme *relaydelay* [17] ou *milter-greylist* [18] pour *sendmail* ou *postgrey* [18] pour *postfix* permettent cette organisation.
7. Les méthodes statistiques telles que l'analyse bayesienne peuvent également être mises en place à ce niveau, à condition de permettre une interaction avec les utilisateurs finaux pour le signalement des faux positifs ou des spams non détectés. Le volume des retours pour l'alimentation de la base de connaissance sera ainsi plus important et la performance du filtrage sera améliorée.

[1] Pour chaque session SMTP entrante, greylist mémorise le triplet (@ip, Mail From, Rcpt). Il génère une erreur temporaire pour les nouveaux triplets

6.2 Le service de messages sortant du domaine

Ce service est parfois négligé en laissant de nombreuses machines du domaine local émettre leurs messages directement vers l'Internet sans aucun contrôle. Une telle configuration peut compromettre gravement la sécurité de votre service de messagerie. En effet, lorsqu'une session SMTP est démarrée, le MTA appelé peut « retourner la communication » et remettre au MTA appelant les messages qu'il aurait en spool pour cette machine. Dès lors certains messages corrompus pourraient franchir les frontières de votre domaine sans être arrêtés ni par le filtrage du port 25 effectué par vos routeurs, ni par les filtrages mis en œuvre sur les MX.

En outre, laisser ce service à la charge des différentes machines de messagerie de votre domaine vous empêche de centraliser les journaux des messages sortants et de les administrer de façon homogène (durée de conservation et autorisation d'accès).

A l'inverse, pour mettre en œuvre une politique centralisée, certains administrateurs trouvent pratique le re-routage transparent disponible sur les routeurs. Cette facilité radicale dispense d'informer les utilisateurs de la bonne configuration des différents MTA, mais ce faisant, elle aggrave le risque juridique pour l'administrateur de messagerie : si une entorse à la déontologie lui était reprochée, par exemple une insuffisance dans la protection de la confidentialité des correspondances, l'absence d'information des utilisateurs sur le re-routage serait une circonstance aggravante. Il est probablement préférable de demander explicitement aux utilisateurs de configurer leur logiciel pour envoyer les messages au serveur de mail sortant. Les journaux des sessions SMTP sortantes refusées par le routeur sont alors un très bon moyen de détection des machines mal configurées ou compromises par un virus ou un *botnet*.

La mise en place de SPF est un argument supplémentaire pour centraliser les trafics sortants de messagerie. En effet, un enregistrement DNS SPF limité aux machines officielles pour ce service permet un meilleur contrôle des usurpations d'identité qu'un enregistrement qui autoriserait par exemple toutes les machines du domaine à émettre des messages vers l'extérieur.

Le plus souvent, parce qu'initialement ce n'était pas indispensable, ce service n'est pas séparé des serveurs de

messages entrants (il est d'ailleurs intéressant de remarquer que l'appellation du DNS « MX » qui désigne les serveurs de messages entrants est ambiguë puisqu'elle fait référence à « *Mail eXchanger* »). Pourtant, il est bien évident que le travail d'un serveur de messages sortants diffère sensiblement de celui des serveurs entrants. Par exemple, le serveur de message sortant a en général des spools importants en particulier du fait de la généralisation de *greylist* alors que le serveur de message entrant devrait conserver des spools minimum en relayant les messages rapidement vers les relais internes servant leurs destinataires.

A bien des égards, il est plus logique de grouper le service de routage sortant avec celui des MSA.

6.3 Le MSA

Le service de soumission de message est un service assez fortement impacté par la lutte contre le spam et les virus.

6.3.1 Le MSA et le filtrage

Tout d'abord, s'il semble évident que le filtrage anti-virus / anti-spam est indispensable sur le flux entrant, l'expérience nous montre qu'il est tout aussi indispensable lors de l'émission des messages. En effet, il convient de protéger votre domaine d'une contagion interne par un virus mais aussi de ne pas propager vers l'extérieur ou dans votre domaine les virus qui affectent certaines de vos machines.

Outre les virus qui se propagent par messagerie et dont on reconnaît une signature dans les messages, certains messages internes de votre domaine peuvent être des spams émis par des *botnets*. Les *botnets* sont des réseaux de *zombies* (PC infectés par des programmes hostiles). Ils sont utilisés comme moteur de diffusion de spam. Les spams propagés ainsi ne sont pas détectés par des anti-virus mais peuvent l'être par des filtres anti-spam à apprentissage.

Les mesures de filtrage sur le MSA peuvent aussi être mises en œuvre sur les serveurs de messages sortants, mais dans ce cas, elles ne protègent pas votre domaine d'une propagation interne.

6.3.2 Le MSA et l'authentification SMTP

Il est acquis depuis longtemps que les utilisateurs du domaine local établissant des sessions SMTP depuis l'extérieur du domaine pour remettre des messages doivent être authentifiés. Cette contrainte résulte des mesures de prévention contre le détournement de vos routeurs SMTP pour l'acheminement du spam (fermeture de l'*open relay* SMTP).

L'émergence de standards d'authentification tel que DKIM, et plus généralement le besoin de maîtriser le respect de la politique de messagerie de l'établissement nous fait penser qu'il faut généraliser l'authentification des sessions SMTP vers les MSA. En effet, le plus souvent c'est le MSA qui signe les messages au format DKIM. Il ne peut le faire à la légère sans être certain de l'identité du *Sender* du message. Cette mesure est facilement compréhensible par les utilisateurs car elle est analogue à ce qui se pratique pour les serveurs POP/S ou IMAP/S, elle est déjà demandée par certains ISP commerciaux et elle permet d'unifier les instructions données aux utilisateurs nomades ou présents dans le domaine local. Un PC portable (configuration la plus fréquente pour les utilisateurs nomades) peut donc être déplacé sans changer sa configuration. Outre le fait qu'elle est indispensable pour respecter l'architecture de DKIM, cette mesure augmente la confiance dans les logs du MSA puisque les informations d'identité sont authentifiées.

6.4 Le service de filtrage

Les techniques de filtrage sont nombreuses (antivirus, blacklist, whitelist, analyse bayesienne…). Le plus souvent elles deviennent intéressantes lorsqu'elles sont corrélées entre elles. Sans une mise à jour régulière, leur efficacité baisse assez vite. Le filtrage est un service dont l'administration est prenante, il est imparfait par nature parce qu'il laisse passer certains spams et est responsable de faux positifs. De ce fait, il peut être refusé par les utilisateurs qui parfois n'hésitent pas à utiliser des arguments juridiques. Il est donc important d'expliquer le fonctionnement des filtres, sans en cacher les effets pervers, et de pouvoir débrayer certains filtres à la demande de chaque usager.

Il y a un grand intérêt à mutualiser le service de filtrage entre différents éléments de l'architecture, par exemple les MX et le MSA (il est particulièrement important que tous les MX du domaine disposent du même niveau de service de filtrage). C'est possible en installant un serveur spécifique qui traitera les messages via une interface SMTP ou milter (dans le cas de sendmail). On peut alors limiter la multiplication des licences de serveur antivirus.

6.5 Le MDA

Le service de dépôt des messages est chargé de la réception des messages provenant d'un MTA et de leur dépôt dans la boite aux lettres des utilisateurs. Sur serveur unix, ce service est assuré typiquement par un programme comme *procmail*.

Dans le processus d'acheminement d'un message, c'est la phase finale avant sa lecture proprement dite par l'utilisateur à l'aide de son MUA. À ce stade, un message a normalement été traité par les outils anti-spam installés en amont. Il a donc été accepté et ne présente pas de caractéristique ayant entraîné son rejet par le système de messagerie mais peut avoir été « marqué » comme spam potentiel.

De par sa proximité avec les utilisateurs, le MDA peut également être candidat pour prendre en charge le filtrage anti-spam préventif.

Ces méthodes impliquent de mettre en place une interaction avec les utilisateurs qui consistera à leur donner les moyens de signaler soit les spams non détectés soit les faux positifs. Les retours des utilisateurs permettront :

- dans le cas de l'utilisation de l'analyse bayesienne, d'alimenter la base de connaissance afin d'améliorer le filtrage des messages ultérieurs
- de manière générale, de prendre en compte les anomalies éventuelles afin de corriger le filtrage, par exemple en changeant la configuration de certains tests.

L'action de l'utilisateur peut être simplement le dépôt des messages dans un dossier particulier ou l'envoi à une adresse de messagerie particulière.

Pour le cas de l'analyse bayesienne, la base de connaissance peut être commune à tous les utilisateurs ou différente pour chacun d'entre eux. Ce choix devra tenir du fait que le volume de messages traités aura une conséquence directe sur la pertinence des résultats obtenus.

6.6 Le MUA

Pour l'utilisateur, le client de messagerie est la partie visible de l'iceberg que constitue le service de messagerie électronique. Certains de ces logiciels, comme *Thunderbird* ou *Outlook*, intègrent des fonctionnalités de filtrage anti-spam s'appuyant sur l'analyse bayesienne.

Chaque message classé comme spam est marqué. Tout spam non détecté peut être marqué manuellement par l'utilisateur. De la même façon, toute détection de faux positifs peut être corrigée par l'utilisateur. Ces deux actions auront pour effet d'alimenter la base de connaissance locale pour un tri futur plus efficace.

Ce filtrage au niveau du MUA donne d'excellent résultats en complément des autres traitements anti-spam au niveau du service de messagerie.

Sa principale faiblesse réside dans la nature très localisée de la base de connaissance. En cas de changement de poste de travail, ou de MUA, on perd la base de connaissance utilisée auparavant.

6.7 Place des utilisateurs nomades dans l'architecture

Le service de messagerie est le premier service demandé par les utilisateurs nomades. L'arrivée du spam pose de nouvelles contraintes pour la mise en œuvre du service. C'est souvent dans ce cas que l'utilisateur dispose d'une connectivité moindre et le volume du spam devient une gêne encore plus importante.

Nous distinguons trois cas de nomadisme :

1. l'utilisateur d'une solution occasionnelle de type « cybercafé ». Il n'a parfois aucun moyen de configurer son environnement et en tout cas jamais le contrôle sur la sécurité du poste qu'il utilise. Dans ce cas, l'utilisation d'un webmail résout de nombreux problèmes. En effet, toutes les opérations de messagerie proprement dite sont effectuées par le logiciel de passerelle entre le mail et le web et sont donc opérées depuis l'intérieur du domaine. L'utilisateur est donc vu comme un utilisateur local et les techniques de type SPF ou DKIM ne sont pas impactées.
2. l'utilisateur dispose d'un VPN, il accède au réseau local à distance. Là encore, du point de vue des services de messagerie, l'utilisateur peut être considéré comme local.
3. l'utilisateur accède au service avec un PC portable ou un PC familial à travers un réseau à priori inconnu. Il peut configurer son outil de messagerie mais il ne dispose pas d'un VPN. Cette situation est de plus en plus fréquente. Dans ce cas, le webmail, solution très appréciée il y a quelques années, l'est de moins en moins. En effet, l'utilisateur aspire à disposer de la même interface que lorsqu'il accède depuis son bureau (avec le même matériel portable dans les cas les plus favorables). Certaines fonctionnalités manquent dans les webmail, par exemple le travail hors connexion avec re-synchronisation des dossiers après coup.

Nous discutons ici du dernier des trois cas de figure. Les services IMAP ou POP ne posent pas de gros problèmes puisque ce sont des services avec authentification. On notera cependant les difficultés liées aux dispositifs de lutte contre le spam situés sur le poste de travail, principalement le filtrage bayesien. En effet, lorsque l'utilisateur change de poste de travail, la base d'apprentissage est chaque fois nouvelle et le bayesien moins efficace avec plus de spam non détecté et surtout, un risque de faux positif plus élevé. Dans ce cas, il est préférable de disposer de filtrage bayésien sur le serveur de consultation, à condition que l'interface permettant d'alimenter ceux-ci reste facile d'accès et personnelle.

De même, les filtres permettant de classer les messages dans différents dossiers (par sujet ou pour séparer le spam du ham) ne sont pas forcément à jour sur les différents postes de travail utilisés.

Concernant l'émission de message, il est souvent recommandé aux utilisateurs nomades d'utiliser le mailhost de leur réseau d'accueil. Cette solution est assez mauvaise. D'une part elle n'est pas pratique pour l'utilisateur qui doit dans chaque cas reconfigurer son MUA (il est rarissime qu'un nom de mailhost soit fourni par le serveur DHCP). Par ailleurs, elle ne permet pas le contrôle de votre politique de messagerie (filtrage des messages sortants).

Rappelons que mettre en place SPF suppose que l'administrateur du domaine connaisse toutes les machines

autorisées à émettre des messages en utilisant le *Mail From :* du domaine. Faute de quoi, SPF sera utilisé en configuration dégradée avec le statut *neutre* comme résultat de tout test SPF négatif. Cette configuration indique qu'il faut traiter les messages non conformes à la déclaration SPF du DNS comme si aucun enregistrement SPF n'existait pour le domaine.

DKIM offre la même possibilité (indiquer qu'il peut exister des messages légitimes non signés) ou au contraire on peut installer un dispositif de signature DKIM sur le MUA nomade. Même si cela devenait disponible pour les MUAs de notre communauté, on retrouverait alors certaines difficultés rencontrées avec les IGC, en particulier la difficulté à déployer et à sécuriser des clés privées sur les postes de travail des utilisateurs.

Il est bien sûr préférable d'ouvrir le service de MSA aux utilisateurs authentifiés du domaine, même si ceux-ci sont géographiquement à l'extérieur du réseau local.

Ce point nous amène à examiner les conditions d'un bon service réseau offert aux utilisateurs nomades de passage dans votre établissement. Le réseau d'accueil sur lequel vous connectez ces utilisateurs occasionnels est en général fermement encadré, mais il ne doit pas filtrer pas les accès SMTP sortants. Pour ce service, les utilisateurs du réseau « invité » sont donc moins contrôlés que ceux de votre établissement.

En effet si vous ne permettiez pas des accès sortant sur le port 25, vous risquez :

- de casser la logique relative à SPF qui peut être déclarée dans le DNS ;
- d'empêcher la signature par DKIM éventuellement prévue par le réseau de votre invité ;
- de rendre impossible l'authentification SMTP prévue.

7 Conclusions

Ces dernières années, le spam a largement dégradé la confiance des utilisateurs dans le service de messagerie. L'efficacité des techniques de lutte contre le spam a tendance à diminuer parce que les spammeurs les contournent. Aussi faut-il périodiquement reconsidérer les armes de lutte employées. Les changements peuvent être périlleux, surtout quand ils sont mis en oeuvre au sein d'une architecture qui ne serait pas adaptée. C'est pourquoi il est important de définir une architecture modulaire du service de messagerie permettant d'intégrer rapidement de nouvelles techniques. Soulignons que cette modularité n'est pas dictée uniquement par l'existence de gros trafics ; elle répond principalement à une logique fonctionnelle et s'applique donc aussi dans des domaines de messagerie de taille modeste. Cette évolution est aussi l'occasion de mettre en cohérence l'organisation technique de la messagerie avec les responsabilités des différents acteurs.

Enfin, elle est rendue indispensable pour réussir le déploiement de DKIM à l'échelle de notre communauté. Il est permis d'espérer que ce type de solution de signature apportera plus de sécurité aux usages basés sur la messagerie.

8 Bibliographie

[1] Phishing, http://www.antiphishing.org/

[2] Botnets, http://en.wikipedia.org/wiki/Botnet

[3] Mail filtering with Joe's j-chkmail, http://j-chkmail.ensmp.fr/

[4] Spamassassin, http://spamassassin.apache.org/

[5] RFC 2554, SMTP/AUTH

[6] RFC 2487, Service Extension for Secure SMTP over TLS SMTP-TLS

[7] RFC 2246, Transport Layer Security (TLS)

[8] Greylisting, http://www.greylisting.org/

[9] Razor, http://razor.sourceforge.net/

[10] DCC, http://www.dcc-servers.net/dcc/

[11] Bogofilter, http://bogofilter.sourceforge.net/

[12] Sender Policy Framework (SPF) http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-02.txt

[13] DKIM, DomainKeys Identified Mail http://mipassoc.org/dkim/index.html

[14] Groupe WG-Antispam, http://www.cru.fr/antispam/

[15] *« Why you shouldn't jump on the SPF bandwagon »*, http://www.advogato.org/article/816.html

[16] François Morris. *« S ignature des message : une réponse contre le spam ? »* Dans *Actes du congrès JRES2005*, Marseille, Décembre 2005

[17] Relaydelay, http://www.cru.fr/antispam/index.html/doku.php?id=relaydelay

[18] Milter-greylist http://hcpnet.free.fr/milter-greylist/

[19] Postgrey, http://www.cru.fr/antispam/index.html/doku.php?id=postgrey