



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Lutter contre le spam

Netsec 2004

30 Mars 2004



Hervé Schauer

<Herve.Schauer@hsc.fr>

www.hsc.fr

- x Spam
- x Serveur de messagerie, Sécurité du poste client
- x Postfix
 - x Description, architecture, anti-spam/anti-relayage, filtrage de contenu, TLS
- x Amavisd-new
- x SpamAssassin
 - x DNSBL, Bases de spams
- x Clamav
- x Administration
 - x Client Unix, client Windows, mises à jour anti-virales et anti-spam
- x Conclusion
- x Références et remerciements

- x Spam ou pourriel : courrier électronique non-sollicité
 - x Commercial, politique, *hoaxs*, etc
 - x Anglophone, francophone, germanophone, chinois, etc
 - x Existe avec le courrier postal, le téléphone, la télécopie, les SMS
- x Le spam de courriel a le meilleur modèle économique que toutes les formes de spam
 - x Le spam ne coûte rien
 - x Le spam rapporte de l'argent au spammeur
 - x Le spam est sans risque pour le spammeur
- x Parce que votre adresse électronique est connue, publiée, vendue, revendue, etc
 - x Beaucoup d'informaticiens utilisent des adresses personnelles jetables
 - x Comment faire dans un organisme, une entreprise ?

- x Le serveur de messagerie ouvert sur Internet doit permettre
 - x Un relayage SMTP sécurisé
 - x Une lutte anti-virus
 - x Une lutte anti-spam
- x Il doit intégrer toutes ces briques
- x La lutte anti-spam est généralement conçue avec des logiciels libres
 - x Les logiciels commerciaux anti-spam réutilisent les logiciels libres
- x Le serveur de messagerie Internet permet de construire une sécurité sur le périmètre de l'entreprise
 - x Il applique une protection sur l'ensemble, quel que soit le contenu, même s'il est mal connu
 - x Il ne constitue qu'un premier rempart de défense

- x La sécurité sur le périmètre ne permet pas de se passer de sécurité sur le poste client
 - x Un anti-virus sur la messagerie oublie tous les autres protocoles véhiculant des virus : HTTP, HTTPS, messageries instantanées, échanges poste à poste
 - x Un PC sous Windows a toujours besoin d'un anti-virus
 - x Un PC sous Windows a toujours besoin d'un firewall
- x La sécurité sur le poste client ne permet pas une sécurité comme sur le périmètre
 - x La sécurité impose une architecture solide : séparation de privilèges, cloisonnement des fonctions, robustesse, administration par un professionnel
 - x La messagerie impose des fonctionnalités d'anti-relayage, de SMTP/TLS
 - x Les contraintes de l'Internet sont incompatibles avec un poste client sous Windows dans un réseau privé d'entreprise

- x Serveur de messagerie sécurisé libre sous Unix/Linux
 - x Commercialisé par IBM (IBM Secure mailer)
 - x Référence des serveurs de messagerie sur Internet
- x Compatibilité maximale avec Sendmail
- x Conçu et écrit dès le départ avec la sécurité dans le cahier des charges
 - Modulaire :
 - ⇒ programmes petits et lisibles
 - ⇒ chaque fonction est isolée
 - Chaque module est restreint au maximum :
 - ⇒ utilisateur postfix
 - ⇒ exécution dans une cage
 - Files d'attente multiples
 - Pas de programme privilégié (SUID)
 - L'architecture est difficile à casser

❑ Mécanismes de sécurité anti-spam

➤ Liste noire :

⇒ Client

- × Adresse IP

- × Nom de domaine

- × Adresse de retour Return-Path :

- × RBL <http://www.mail-abuse.org/rbl/>

- × Absence d'enregistrement inverse dans le DNS

➤ Autres :

⇒ Utilisation d'expressions rationnelles dans les entêtes des messages

- × Arrêt de certains virus jusqu'à ce que la base anti-virale soit mise à jour

- × Interdiction temporaire de certaines extensions de fichiers

 - bagle, mydoom, netsky...

⇒ et dans le corps des messages

❑ Mécanisme anti-relayage

➤ Vérification de l'adresse IP cliente ou du RCPT TO:

□ Possibilités de filtrage via l'interface `content_filtering`

- “ *Simple content filtering* ” : script de filtrage réexécutant la commande `sendmail` pour réinjecter le message “ marqué ”
- “ *Advanced content filtering* ” : postfix exécute 2 démons `smtpd`, le marquage est effectué par un relais smtp tiers
- Voir le fichier `FILTER_README` dans la distribution.

□ Il est possible d'utiliser avec le filtrage de contenu avancé :

- Un relais SMTP anti-virus commercial
- Une “ *glue* ” qui communique en SMTP et utilise des outils tiers
 - ⇒ ex : `amavisd-new` utilisant `Mail::SpamAssassin` et plusieurs anti-virus dont `clamav`
- L'envoi en LMTP vers le relais filtrant permet d'avoir des résultats différents pour chaque destinataire
 - ⇒ Postfix peut alors générer lui même les avis de non distribution nécessaires
 - ⇒ sinon c'est le relais filtrant qui doit les générer
- Plus tard : ICAP, OPES ?

- ❑ Le chiffrement se fait entre deux serveurs
- ❑ SMTP-TLS n'est pas une encapsulation de SMTP dans TLS :
 - Le serveur contacté émet l'annonce STARTTLS
 - Le client envoie la commande STARTTLS
 - Négociation TLS entre les deux parties
 - Session SMTP normale dans le flux TLS
 - Retour à la bannière (EHLO) à la fin de chaque message
- ❑ TLS permet :
 - D'authentifier un utilisateur à partir d'un certificat client
 - D'imposer un certificat valide dans un réseau privé
 - De permettre le relayage depuis et vers l'Internet si le certificat est valide
- ❑ Voir <http://www.hsc.fr/ressources/breves/postfix-tls.html>
 - Comment patcher postfix et configurer la partie TLS

- Démon en perl permettant d'appliquer un filtrage de contenu
 - À un flux SMTP
 - Anti-virus et anti-spam
 - <http://www.ijs.si/software/amavisd/>
- Utilise le module Mail::SpamAssassin pour détecter les spams
- Sait utiliser de nombreux anti-virus :
 - Démons ou ligne de commande
 - Commerciaux et libres.
- Développé pour :
 - Limiter les risques de perte de mails
 - ⇒ ne prend jamais la responsabilité d'un mail
 - ⇒ ne modifie pas les messages :
 - * ajoute un entête, met en quarantaine, rejette ou émet un avis de non délivrance
 - Optimiser les flux
 - ⇒ peut traiter plusieurs messages simultanément
 - ⇒ garde un cache des derniers résultats pour ne pas retraiter le même message

- ❑ Logiciel libre de filtrage en perl (Unix/Windows)
 - <http://www.spamassassin.org/>
- ❑ Permet de détecter les spams à partir d'un système de notations
 - Utilise de nombreux tests de types différents, chacun possédant un certain score
 - Les scores sont calculés pour maximiser le taux de détection (>>95%) tout en minimisant les risques de faux positifs (<<0,1%)
- ❑ Marque les message du score
 - X-Spam-Status :
 - X-Spam-Level :
 - Dans le sujet

- ❑ Logiciel libre de qualité professionnelle :
 - McAfee SpamKiller Technology “ *Powered by McAfee SpamAssassin* ”
- ❑ Peut être utilisé
 - Par un utilisateur final depuis procmail ou via un relais pop3
 - Dans un relais SMTP via le module Mail::SpamAssassin
- ❑ Attention : le filtrage anti-spam peut prendre beaucoup de ressources
 - Mémoire, temps de calcul

- ❑ Une DNSBL est une *Black List* DNS :
 - Toutes les adresses IP que le serveur connaît sont suspectes
- ❑ Les natures des adresses IP peuvent différer :
 - Adresses IP d'où des spams ont été envoyés
 - Adresses IP de serveurs relais ouverts sur Internet
 - Adresses IP de clients de FAI sur des plages d'adresses dynamiques
 - Etc.
- ❑ Les politiques de gestion de ces listes diffèrent :
 - Modalités d'entrée/sortie, réactivité, etc.
- ❑ SpamAssassin et postfix peuvent tous les deux utiliser des DNSBL
- ❑ Site de test : <http://www.dnsstuff.com/>
- ❑ Listes de DNSBL : <http://www.moensted.dk/spam/> et <http://www.declude.com/junkmail/support/ip4r.htm>

- ❑ Des bases de spams sont confectionnées de façon collaborative
 - Grâce à la collaboration de ses utilisateurs.

- ❑ Chaque message reçu est comparé à une base centrale
 - Entre le “ *client* ” et le “ *serveur central* ” seuls des “ *hashs* ” sont échangés.

- ❑ Certains systèmes permettent de détecter des spams “ *mutants* ”
 - en comparant des parties de messages

- ❑ Certains systèmes utilisent un “ *niveau de confiance/spammicité* ”

- ❑ De telles bases sont Razor, Pyzor et DCC
 - SpamAssassin sait les utiliser toutes les trois.

- ❑ Anti-virus libre destiné à filtrer les messages électroniques
 - <http://www.clamav.net>
- ❑ Peut aussi être utilisé en ligne de commande pour scanner une arborescence
 - Sous Linux un module noyau (en cours de développement) permet de scanner tout fichier lors de son ouverture et d'en interdire l'accès s'il est infecté.
- ❑ Un démon clamd permet d'optimiser les performances en n'initialisant le moteur qu'une seule fois.

- ❑ La priorité est portée sur la mise à jour des virus au fur et à mesure des nouvelles apparitions aidés par des ISP pour les détecter
 - mais la base est aussi complétée avec les anciens virus qui ne sont plus (ou peu) en activité.
- ❑ Le support des fichiers office (word, excel...) est toujours désactivé

- ❑ Pour les clients Windows il est possible d'y utiliser un relais
 - POP3 : <http://mcd.perlmonk.org/pop3proxy/>
 - IMAP : <http://sourceforge.net/projects/imapassassin>
- ❑ Requièrre d'installer SpamAssassin sous Windows :
 - <http://www.openhandhome.com/howtosa.html>
- ❑ Il existe aussi des programmes et plugins payants :
 - Bloomba et SAproxyPro : <http://www.statalabs.com/>
 - Plugin eudora : <http://www.spamnix.com/>
 - SpamKiller : <http://www.nai.com/>

- Les deux systèmes de filtrage de contenus installés doivent être mis à jour régulièrement pour s'adapter aux nouveautés.

- Pour clamav, lancer la commande *freshclam*
 - soit en mode démon
 - soit depuis la crontab de l'utilisateur amavis

- Il est aussi possible de déclencher la mise à jour lors de la réception d'un mail dans la liste clamav-virusdb@lists.sourceforge.net

- ❑ Pour SpamAssassin l'utilisation des DNSBL et des bases de spams permet de faire contrepoids aux bases de règles statiques.
- ❑ Il est tout de même possible d'utiliser des bases de règles générées par d'autres personnes
 - le script *my_rules_du_jour* permet de télécharger plusieurs listes de ce type :
 - ⇒ <http://www.exit0.us/index.php/RulesDuJour>
- ❑ Attention : il est important de vérifier que des jeux de règles tiers utilisés ne génèrent pas de faux positifs
 - pour cela il faut essayer ces règles sur deux corpus de hams et spams, représentatifs des mails reçus et datant de moins de 6 mois
 - par exemples *chickenpox.cf* et *tripwire.cf* peuvent être la cause de faux positifs sur de longs mails en français
 - les raisons des faux positifs avec l'utilisation de nouvelles règles sont :
 - ⇒ que les scores du nouvel ensemble de tests n'ont pas été recalculés en incluant les nouvelles règles
 - ⇒ les corpus de hams utilisés pour tester les nouvelles règles sont souvent non significatifs des hams reçus par des tiers.

- x Il est possible de construire une architecture de messagerie efficace
 - x Les virus et les spams sont éliminés ou marqués pour l'utilisateur
- x La vie de l'utilisateur est améliorée
 - x C'est lui qui décide suivant les marques de l'anti-spam
- x La lutte est sans fin
- x Il existe d'autres possibilités
 - x Sous-traiter le travail de filtrage à un opérateur
 - x De plus en plus de fournisseurs d'accès le proposent

- x Important

- x Déployer un anti-virus sur les postes de travail
- x Prévoir une mise à jour automatique des anti-virus
 - x A la fois sur le périmètre et sur les PC
- x Quand un spam ou un virus est détecté : ne jamais envoyer d'avis de non-délivrance à l'extérieur

www.hsc.fr

- x Elements de réflexion sur le spam, Hervé Schauer, HSC, 01/04, Groupe de contact sur le spam
<http://www.hsc.fr/ressources/presentations/ddmspam/>
- x Généralités sur le spam, Stéphane Bortzmeyer, AFNIC, 01/04, Groupe de contact sur le spam
<http://www.afnic.fr/data/divers/public/generalites-sur-le-spam.pdf>
- x Serveur de messagerie sécurisé et libre, Denis Ducamp, 02/04, Séminaire 01Réseaux
<http://www.hsc.fr/ressources/presentations/SrvMessagSecLib/>
 - x Précise notamment les aspects installation et mise en oeuvre
- x Présentation de SpamAssassin, Denis Ducamp, 11/02, OSSIR Resist
<http://www.hsc.fr/ressources/presentations/spamassassin/>

- x Wietse Venema pour avoir écrit Postfix
- x Denis Ducamp, co-auteur de la présentation, et pour ses présentations précédentes