Le filtrage de mail sur des « gros » serveurs

http://j-chkmail.ensmp.fr

Jose-Marcio.Martins@ensmp.fr

Ecole des Mines de Paris

Plan

- Les serveurs importants...
- Ce qui se passe sur un gros site
- j-chkmail – les idées
- Conclusions

Avertissement

- Les citations à d'autres logiciels paraissant dans cette présentation n'ont pas pour but la comparaison de l'efficacité/qualité, mais plutôt la présentation des différences d'approche des solutions. Ces autres solutions étant largement diffusées, elles sont certainement très efficaces.

Les « gros » serveurs...

- Plusieurs milliers d'utilisateurs
- Plusieurs centaines de milliers de messages par jour
- Plusieurs gigaoctets traités par jour

Les « gros » serveurs...

- Structure non-specialisée ouverte : université, ...
- Structure spécialisée ouverte : département d'une université
- Structure specialisée opaque : industrie, ...
- Hébergeur de comptes – hotmail, yahoo, pobox, ...
  - Gratuit, pas de rapport contractuel, ...
- Fournisseur d'accès – wanadoo, free, ...
  - Payant, rapport contractuel, ...

Le filtrage sur des « gros » serveurs
L'efficacité

- Population souvent hétérogène : infirmière, acheteur, communication, informaticien...
  - Typologie variée des boites aux lettres, ainsi que des spams.
- Nombreux utilisateurs, souvent inconnus de l'administrateur de la messagerie
  - Plus difficile d'évaluer/corriger l'efficacité du filtre

Quid des probabilités de détection et d'erreur ???

Sur l'efficacité du filtrage...
La réalité sur les tests statistiques

- 99% is only true for personal email
- Statistical techniques learn what your personal email looks like
- Doesn't work quite as well when you have users with dissimilar inboxes
- Live data testing accuracy about 80 – 95%

Source : Matt Sergeant, Internet-Level Spam Detection and SpamAssassin 2.50, Spam Conference 2003 : http://spamassassin.apache.org/presentations/SpamConf2003.pdf

- Conclusion : est-ce bien la peine de calculer avec précision des scores qui ne sont que des approximations ???

Le filtrage sur des « gros » serveurs
Les aspects liés au serveur

- Extensibilité
  - Si : Volume V -> 1 serveur
  - Alors : Volume k*V -> k serveurs / processeurs ?

  Utiliser au maximum les ressources des serveurs, tout en laissant une marge de sécurité
- Sécurité – cible plus recherchée
- Fiabilité – minimiser les arrêts de service (en nombre et durée), tolérance aux fautes, ...
- Limitations du système d'exploitation

Limitations du système d'exploitation

- IOPS – Fichiers créés/supprimés par seconde
  - Minimiser le nombre de fichiers temporaires
  - Spool du filtre dans un disque dédié
  - Spool dans des disques SSD (Solid State Disk)
- Nombre de processus/threads

    N = taux d'arrivées x temps de séjour (loi de «Little»)
  - Des centaines de threads/processus aussi bien pour le MTA que pour le filtre
  - Minimiser le temps de traitement, même si c'est de l'attente
  - Libmilter avec « pool of workers »
    http://j-chkmail.ensmp.fr/libmilter
- ...

(Parenthèse : le protocole SMTP)

```
    martins@calloway:~> telnet paris smtp
    Trying 194.214.158.200...
    Connected to paris.
    Escape character is '^]'.
<-  220 paris.ensmp.fr ESMTP Sendmail 8.12.8/8.12.7/JMMC
->  helo calloway.ensmp.fr
<-  250 paris.ensmp.fr Hello calloway [194.214.158.171], pleased to meet you
->  mail from:joe@ensmp.fr
<-  250 2.1.0 joe@ensmp.fr... Sender ok
->  rcpt to:martins
<-  250 2.1.5 martins... Recipient ok
->  rcpt to:tartonpion
<-  550 5.1.1 tartonpion... User unknown
```

Enveloppe

```
->  data
<-  354 Enter mail, end with "." on a line by itself
->  From: Antoine
->  To: Sebastien
->  Subject: test telnet
->
->  C'est un test, je dis !
->  .
<-  250 2.0.0 h2QBmFBx017626 Message accepted for delivery
->  quit
<-  221 2.0.0 paris.ensmp.fr closing connection
    Connection to paris closed by foreign host.
    martins@calloway:~>
```

Corps du Message

Ce qui se passe sur un grand site...

SUR 440.000 MESSAGES

# 1	127535	URIBL_WS_SURBL
# 2	127101	URIBL_SBL
# 3	125917	URIBL_JP_SURBL
# 4	120728	URIBL_OB_SURBL
# 5	96849	BAYES_99
# 6	95827	RCVD_IN_BL_SPAMCOP_NET
# 7	90406	HTML_MESSAGE
# 8	71017	URIBL_SC_SURBL
# 9	46927	MIME_HTML_ONLY
#10	36806	URIBL_AB_SURBL
#11	33822	RCVD_IN_XBL
#12	30930	MIME_BOUND_DD_DIGITS
#13	30649	MPART_ALT_DIFF
#14	28472	URIBL_AH_DNSBL
#15	26638	RCVD_IN_SORBS_DUL
#16	26621	DRUGS_ERECTILE
#17	26394	MSGID_FROM_MTA_HEADER
#18	24615	RCVD_IN_DSBL
#19	23977	MSGID_FROM_MTA_ID
#20	23690	RCVD_IN_SORBS_SPAM
#21	22457	RCVD_IN_NJABL_DUL
#22	21115	RCVD_IN_NJABL_PROXY
#23	21013	RCVD_IN_SBL
#24	20262	X_MESSAGE_INFO
#25	18044	HTML_FONT_BIG

...

Listes noires IP

Listes noires URI

Filtrage bayesien

Heuristiques

Merci à Raymond Dijkxhoorn

On remarque, pour ce filtre...

- Tous les tests sont toujours exécutés (quelques centaines)
- Très peu de critères suffisent pour détecter presque tous les SPAMs
- Les critères les plus pertinents sont des critères externes (listes noires) ou Bayesiens
- Des critères peu fiables en tête (HTML_MESSAGE)

A propos des listes noires IP (RBL)

- Vérification faite au moment de la connexion
- Dépendance externe
- Temps de réponse varie entre quelques milisecondes à plusieurs secondes
- Taux de détection ~ 50 % des messages indésirables
- Taux d'erreur assez variable
- Des listes libres et des listes payantes : dsbl.org, ordb.org, mail-abuse.org
- Multiplier les listes noires n'est pas toujours utile – le gain marginal est faible.
- Sur un gros serveur, si la liste est fiable, parfois il vaut mieux rejeter le message que le marquer.

A propos des listes noires URI

- Recherche dans le corps du message
- La liste la plus répandue est SURBL – www.surbl.org
  - Taux de détection > 80 %
  - Taux de faux positifs < 0.5 %
  - Délai de mise à jour très faible (qques heures)
- Implémentée dans SpamAssassin et j-chkmail

On reviendra...

j-chkmail - Quoi ?

- Filtrage viral (type de fichier + interface externe)
- Filtrage de SPAM
- Aide à la protection du serveur de mail
- Surveillance en temps réel
- Commande du filtre

- Sendmail + API libmilter
- Ecrit en langage C

j-chkmail

- Filtrage comportemental
  - Dégrossir le trafic
  - Cadence de connexion, Spamtraps, « Harvest »...
  - Les messages sont rejetés/marqués sans vérification du contenu

- Filtrage de contenu
  - Affiner le filtrage
  - Recherche de certaines expressions regulières
  - Filtrage d'URLs
  - Heuristiques : forme des messages, conformité, ...
  - Un score est attribué et les messages sont marqués

Extensibilité du filtre

- Pour un trafic N (utilisateurs, messages..)
  - Charge CPU : **L** %
  - Occupation Mémoire : **M** Moctets
- Pour un trafic k x N
  - Charge CPU : f(k,L) %
    - f(k,L) = k * L –> c'est intuitif
    - f(k,L) > k * L –> mauvais
    - f(k,L) < k * L –> ce serait bien – on va essayer
  - Occupation Mémoire : g(k,M) Moctets
    - g(k,M) < k * M –> ce serait bien

Extensibilité de la « charge »

- L'idée : utiliser le historique dans le filtrage
  - Future belongs to those who have the longest memory (Nietzche)
  - Mais il ne faut pas encombrer la mémoire avec un contenu inutile (Joe)
- Historique
  - N'enregistrer que ce qui est utile
  - Listes noires dynamiques – clients avec « mauvais » comportement
  - Rejet de la connexion sans traitement du contenu
    (C'est gagné pour l'extensibilité de la charge !!!)

Utilisation de l'historique (mémoire)
Filtrage comportemental

- Historique court – ~ 20 minutes – en mémoire
  - Cadences : connexion, bounce, ...
  - Rejet des clients trop «gourmands»
  - Abus, DoS, contrôle de charge
- Historique moyen – ~ 4 heures – en mémoire
  - Comportement : «harvest», pots de miel, ...
  - Rejet des clients qui font trop d'erreurs
  - AntiSpam
- Historique long – sur disque
  - SPAMS confirmés
  - Scripts externes -> Blacklistes DNS (pour les MXs)

Filtrage du contenu

- Le but n'est pas quantitatif, mais qualitatif : faciliter le classement par l'utilisateur
- Filtrage plus sévère compensé par «blanchiment» effectué par l'utilisateur (utilisateurs connus, ...)
- Résultats :
    - Score attribué aux messages, indiqué dans un en-tête
    - Message refusé si score important
    - Le client de messagerie du destinataire dirige le message vers une « boite à SPAM » si l'émetteur est ***inconnu*** et si le score dépasse un seuil

Filtrage du contenu – le fond

- Recherche d'expressions regulières
  - Ex :
    - get.*(doctorate|university).*diploma -> mauvais
    - get.{1,30}(doctorate|university).{1,30}diploma -> mieux
  - Temps de traitement important
  - Pas plus de quelques centaines d'expressions
- Recherche d'URLs
  - Extraction du nom de domaine des URLs
    - http://euyiure:ryu;@ehjkr.freeporn.org
  - Le message est traité une seule fois
  - Extremement rapide (< 1 ms par message)
  - Liste noire avec 150000 URLs.

Filtrage du contenu – la forme

- Privilégier les algorithmes rapides
- Critères pertinents et peu nombreux – (< 30) : conformité, entropie, balises HTML «indésirables», ...
- Pas de critères avec score négatif
  - Évolution monotone du score
  - Arrêt à l'atteinte d'un seuil
  - Compromis faux positifs/blanchiment par utilisateur
  - Pas d'erreur de «blanchiment» (cas PGP)
- Les scores sont évalués approximativement (mais pas trop) selon sa « gravité »

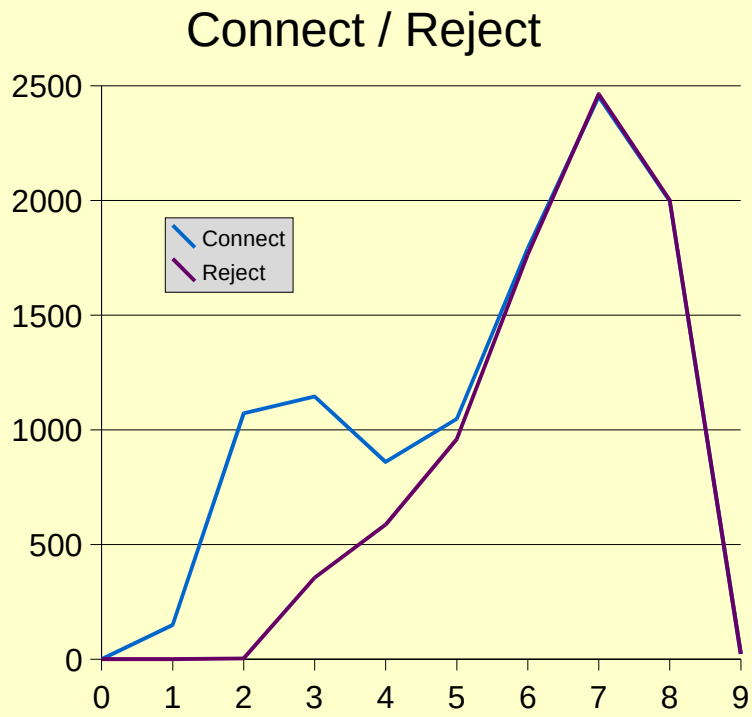
j-chkmail - Protection du serveur...

- Filtre auto-régénérant (increvable)
  - Le filtre se relance en cas de problème
- Mesure de cadence de connexion (par client SMTP)
- Contrôle du nombre de connexions ouvertes (par client SMTP)
- Prise en compte des ressources disponibles (charge CPU, descripteurs de fichiers, ...)

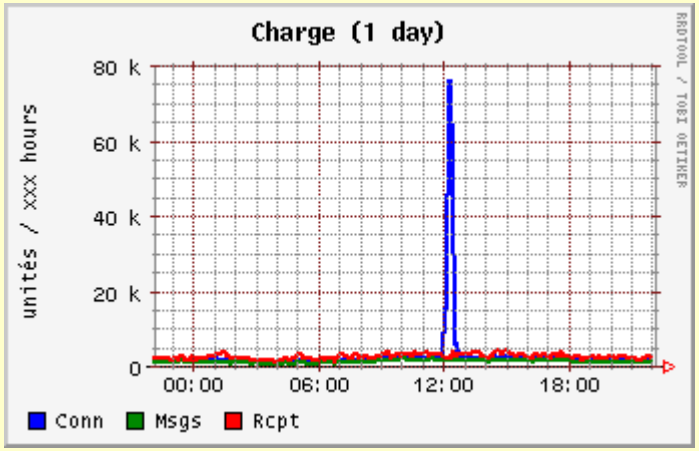
Résultats – mesure de cadence de connexion

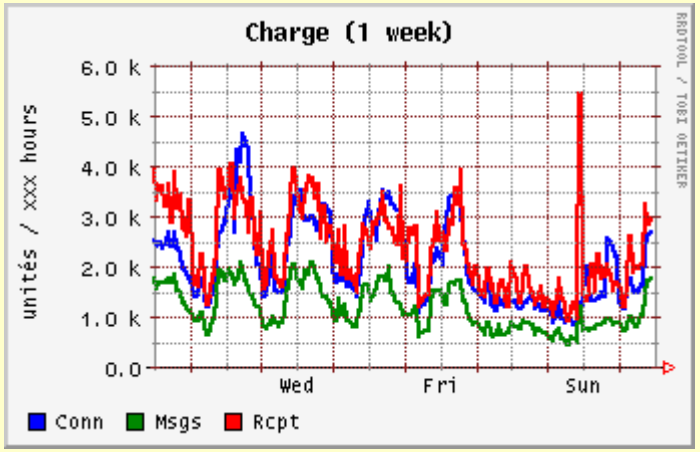
- 10536 connexions en 8 minutes
- 238 clients du réseau 66.216.119.0/24
- Connexions par client : [28 – 67]
- Pic : 86 connexions dans la même seconde
- 15 messages refusés par le contenu, dans les 3 premières minutes

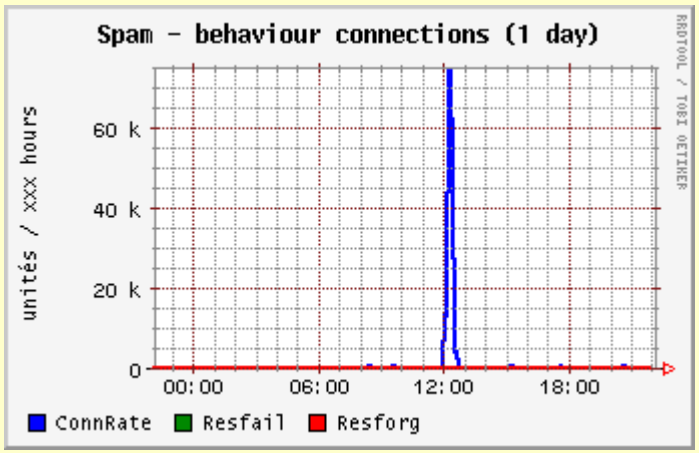
  `www.rapiddealsbyemail.com`
- 8156 connexions refusées par la mesure de cadence de connexion
- Le reste pour des destinataires inconnus (erreur d'adresse)
- **Aucun message légitime perdu ! : "QoS de pauvre »**

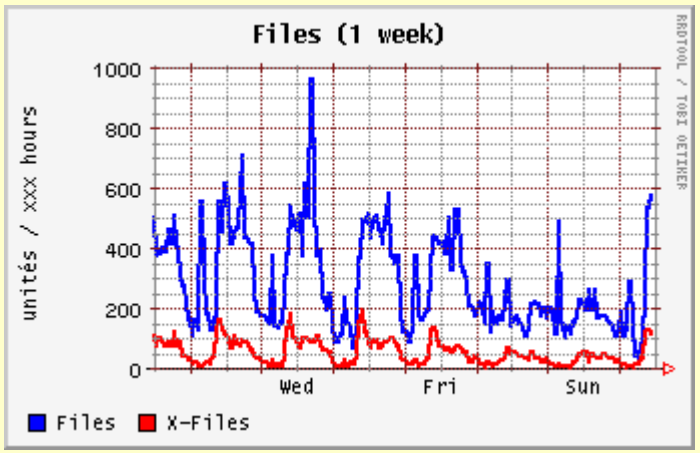


j-chkmail - Surveillance









j-chkmail - Surveillance

```
martins@paris:~> j-printstats -q -l 6h | more
Version                          : Joe's j-chkmail v1.7 - PreAlpha 6
*** Summary
*** TOTAL
 First Connection  : Sun Jun  6 17:33:11 2004
 Last Connection   : Sun Jun  6 23:33:09 2004
 Connections       :    9393
 Gateways          :    4258
 Throttle Max      :     445 / 10 min (for the server)
 Throttle Max      :     100 / 10 min (for a single gateway)
 Duration (sec)    :   0.005  16.931 7226.787 206.110 (min mean max std-dev)
 Work (sec)        :   0.001   0.028    1.803   0.150 (min mean max std-dev)
 Mean Throuput     :   0.647 KBytes/sec
Counts
 Messages          :    5471
 Volume            :  105393 KBytes
 Mean Volume       :   18.81 KBytes/msg
 Recipients        :    8256
 Bad Recipients    :    2145
 Yield             :    0.58 msgs/connection
 Yield             :    0.88 rcpt/connection
 Files             :     672
 X-Files           :     388
 Virus             :       0
```

Surveillance ...

```
martins@paris:~> j-printstats -q -l 6h -m c
                    CONN   MSGS REG.EXP  ORACLE
...
. 24.17.181.231   :     2     1       1       1 : c-24-17-181-231.client.comcast.net
. 24.17.211.202   :     1     1       1       1 : c-24-17-211-202.client.comcast.net
. 24.19.30.98     :     2     4       4       4 : c-24-19-30-98.client.comcast.net
. 24.19.33.250    :     1     1       1       1 : c-24-19-33-250.client.comcast.net
. 24.19.125.53    :     1     1       1       1 : c-24-19-125-53.client.comcast.net
. 24.19.212.106   :     2     1       1       1 : c-24-19-212-106.client.comcast.net
. 24.19.226.165   :     1     1       1       1 : c-24-19-226-165.client.comcast.net
. 24.20.26.47     :     1     1       1       1 : c-24-20-26-47.client.comcast.net
. 24.20.103.148   :     1     1       1       1 : c-24-20-103-148.client.comcast.net
. 24.20.172.173   :     2     1       1       1 : c-24-20-172-173.client.comcast.net
. 24.21.24.32     :     1     1       0       1 : c-24-21-24-32.client.comcast.net
. 24.21.143.163   :     6     1       1       1 : c-24-21-143-163.client.comcast.net
. 24.21.252.100   :     1     1       1       1 : c-24-21-252-100.client.comcast.net
. 24.24.107.127   :     2     1       1       1 : cpe-024-024-107-127.midsouth.rr.com
. 24.24.234.17    :     4     2       0       2 : cpe-24-24-234-17.socal.rr.com
. 24.25.4.97      :     1     1       0       1 : ncmx03.mgw.rr.com
. 24.25.37.146    :     3     2       1       2 : ilm25-37-146.ec.rr.com
. 24.26.180.239   :     1     1       1       1 : CPE-24-26-180-239.mn.rr.com
. 24.28.193.149   :     3     1       0       1 : vamx03.mgw.rr.com
. 24.29.47.228    :     1     1       1       1 : alb-24-29-47-228.nycap.rr.com
. 24.30.28.172    :     1     2       2       2 : c-24-30-28-172.mw.client2.attbi.com
. 24.30.84.80     :     1     1       1       1 : c-24-30-84-80.mw.client2.attbi.com
```

j-chkmail - Commande

```
martins@paris:~> telnet localhost 2010
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
200 OK - Waiting for commands !
reload databases
200 OK for RELOAD DATABASES !
200 URLBL : OK
200 RELOAD DATABASES done !

200 OK - Waiting for commands !
stats connopen
200 OK for STATS CONNOPEN !
*** Open connections :
  170.171.252.28    :   1 : silas.randomhouse.com
  193.251.37.182    :   2 : ASt-Lambert-109-2-4-182.w193-251.abo.wanadoo.fr
  193.49.22.101     :   1 : evry
  220.112.147.75    :   1 : [220.112.147.75]
  64.53.226.128     :   1 : d53-64-128-226.nap.wideopenwest.com
  83.130.129.80     :   1 : IGLD-83_130_129_80.inter.net.il
    6 entries on database
200 STATS CONNOPEN done !
Connection to localhost closed by foreign host.
martins@paris:~>
```

Quelques résultats

- ensmp.fr
  - 2000 utilisateurs, 60000 connexions par jour
  - 1 Sun E280R, Solaris 9, 2 processeurs 900 Mhz
  - j-chkmail

```
   PID %CPU %MEM   VSZ   RSS    SZ  CLS     LWP NLWP PSR S COMMAND
  8354  0.0  0.1  5688  1808   711   TS       1    1   - S /usr/sbin/j-chkmail
 28872  0.9  0.5 19072 18352 2384   TS       1    9   - S /usr/sbin/j-chkmail
```

- jussieu.fr
  - 50000 utilisateurs, 500000 connexions par jour
  - 4 machines sous FreeBSD, 2 processeurs
  - j-chkmail + milter-greylist + Sophos

```
 PID USERNAME  PRI NICE   SIZE    RES STATE  C   TIME   WCPU    CPU COMMAND
 1827 smmsp     96    0 29172K 26772K select 0  40:45  3.52%  3.52% j-chkmail
```

- pobox.sk
  - 20000 connexions par l'heure
  - 1 Sun x86, 2.8 GHZ, sous Linux
  - j-chkmail + clamd

Conclusions

- Filtre rapide et efficace
- Evolution en cours : améliorer la qualité de la détection et la facilité de mise en oeuvre.
- La principale difficulté pour le déploiement, dans une structure comme la notre, est la communication avec l'utilisateur : le « mode d'emploi »

Autres filtres français anti-SPAM

- Spam Oracle – Xavier Leroy – INRIA
  - Filtre bayesien orienté utilisateur, utilisable avec procmail, ou comme plugin pour Kmail
    - http://cristal.inria.fr/~xleroy/software.html
- Milter-greylist – Emmanuel Dreyfuss
  - Implementation de greylisting de Evan Harris pour sendmail
    - http://projects.puremagic.com/greylisting/
    - http://hcpnet.free.fr/milter-greylist