Le spam
introduction

Laurent Aublet-Cuvelier
Renater

Laurent.Aublet-Cuvelier@renater.fr

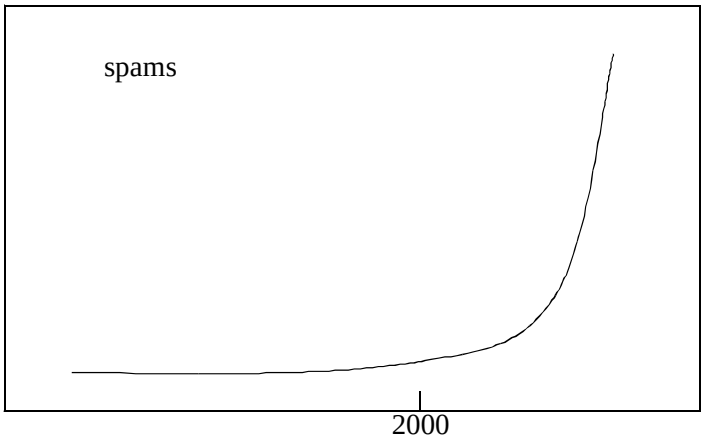
Sommaire

- Introduction
- Le spam
- Les méthodes
  - Principes
  - Exemples
- Conclusion

Introduction

- Le courrier électronique à l'origine
  - SMTP : ***Simple*** Mail Transfer Protocol
  - Principe Internet : interopérabilité
    - Strict sur ce qu'on envoie,
    - Souple sur ce qu'on reçoit !
  - Internet de confiance :
    - « entre gens de bonne compagnie »
- Aujourd'hui :
  - Messagerie instantanée , forums, etc.
    - Tél. mobile, I.M., réseaux sociaux, etc.

Introduction



Sommaire

- Introduction
- Le spam
- Les méthodes
  - Principes
  - Exemples
- Conclusion

Le spam

- spam (pas SPAM)
- spam = message non sollicités
- Activité lucrative !
- C'est illégal…
  - Principe du « consentement préalable » (opt-in)
- Mais !
  - Des exceptions
    - Notion de « collecte loyale » des adresses
    - Notion d'adresse professionnelle
  - Internet = International

Le spam

- Malveillant
  - Arnaque (scam, ...)
  - Fraude (commerce de pillules, …)
  - Déni de service
  - Usurpation d'identifiant (phishing, …)
  - Infections (« Malware », …)
  - Etc.
- « Commercial »
  - Cf. boîte aux lettres « physique »

Le spam

- Cela représente la majorité du trafic SMTP
  - 75 à 95 % selon les sources
  - C'est une pollution :
    - Pour l'utilisateur (BaL débordante)
    - Mais aussi pour les ressources informatiques
      - Réseau, stockage, CPU, etc.
- Notion de courrier « indésirable »
  - Varie d'un individu à l'autre :
    - mutualisation vs spécialisation

Sommaire

- Introduction
- Le spam
- Les méthodes
  - Principes
  - Exemples
- Conclusion

Les méthodes : principes

- La lutte antispam :
  - Eliminer les spams en recus
  - Eviter d'émettre des spams
  - ➢Assurer une bonne qualité du système de messagerie

Les méthodes : principes

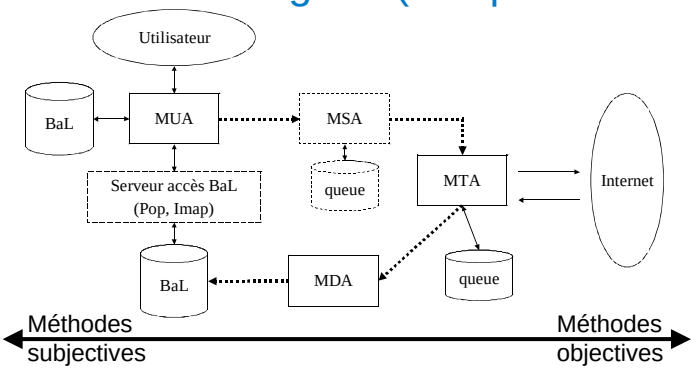
En premier lieu :

- Bonne gestion de son domaine
  - Architecture maîtrisée
    - Pas de solution universelle
    - Mais des bonnes pratiques : passerelles, etc.
  - Gestion des nomades (MSA authentifiés)
    - Impact sur les traitements côté destinataire
  - Information des utilisateurs

– But
  - Ne pas envoyer de spams
  - Donner confiance aux destinataires
  - Eviter d'en recevoir

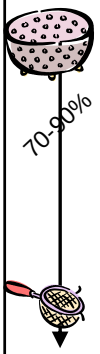
Les méthodes : principes

- Possibles sur les différents maillons de la chaîne de messagerie (complémentaires) :

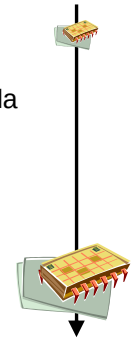


Les méthodes : principes

- Typologie
  - Listes noires et blanches

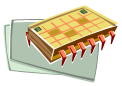


  - Sur la source :
    - Listes de réputations
    - Vérification (voire authentification) de la légitimité de la source
  - Analyse comportementale
    - Nombre de messages émis, de destinataires
    - Respects des protocoles, normes, etc.
  - Analyse du contenu



Les méthodes : principes

- Analyse de contenu
  - Sur les entêtes et le corps



  - Heuristiques
    - Ensemble de règles sur le contenu, la forme, etc.
      - Attribut un score (seuil de spam)
  - Signatures
    - Base de signature (à la manière des anti-virus)
  - Statistiques
    - Ex. classification bayésienne
    - Nécessite un apprentissage

    => Boucle de feedback avec l'utilisateur

Sommaire

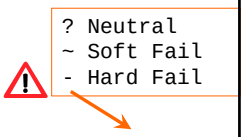
- Introduction
- Le spam
- Les méthodes
  - Principes
  - Exemples
- Conclusion

Les méthodes : exemples

- Listes de réputations
  - RBL (Realtime Blackhole List)
  - DNSBL (DNS-based Black List)
  - Liste d'adresses IP
    - Relais ouverts, sources de spams, etc.
    - Un élément de choix important !
  - Consultation via mécanisme DNS
    - Tester 198.51.100.12
      = résoudre 12.100.51.198.myrbl.tld.
  - Nombreuses offres : **choix délicat**
    - Pertinence/Réactivité/Politique/Coûts
    - Utilisation : bloquage smtp, score, etc. ?

Les méthodes : exemples

- SPF
  - Sender Policy Framework
  - Un enregistrement TXT dans le DNS
    - Pour un domaine, décrit les émetteurs (machines) légitimes
  - Controversé, et pas si simple
    - Forwarding (SRS)
  - Utilisation
    - Meilleure confiance
  - Exemple



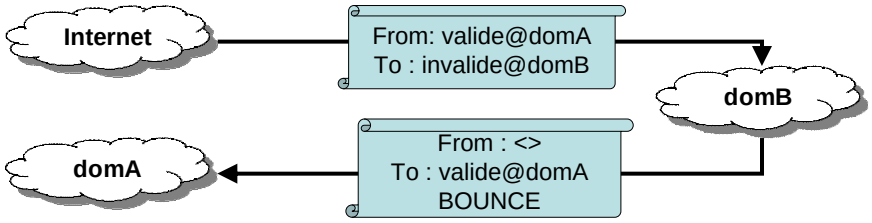

```
example.net   IN     TXT    "v=spf1 mx a:listes.example.net ?all"
```


Les méthodes : exemples

- DKIM
  - Principe
    - Signer tout ou partie des mails sortant de son domaine
    - Permet d'authentifier la provenance du mail à l'arrivée
    - Architecture non intrusive
      - Pas d'architecture de clé complexe (clé de domaine dans le DNS (avec sa politique « DKIM »)
      - Transparent pour l'utilisateur
        - » Signature par MSA, vérification par MDA par exemple
  - Attention : n'indique en rien la « qualité » du mail

Les méthodes : exemples

- Basckscattering
  - Principe d'envoi de spam par rebond



  - Parades
    - DomB : minimiser la génération de « bounces »
      - absolument résoudre les « user unknown » en session
    - DomA : BATV (marquages des mails sortants)

Sommaire

- Introduction
- Le spam
- Les méthodes
  - Principes
  - Exemples
- Conclusion

Conclusion

- Le filtrage du spam
  - Agrégation et association de méthodes de luttes
- Le problème
  - Eviter les pertes : faux positifs
  - Mais limiter les faux négatifs !
    - Méthodes les plus sûres : rejet
    - Méthodes moins sûres : marquage

Conclusion

- La lutte contre le spam
  - Un jeu permanent du chat et de la souris
    - Technique
    - Juridique

  => Une tâche jamais terminée…
    - 100 fois sur le métier…
  - De plus en plus une affaire de spécialiste
  - La mutualisation permet de soulager
    - Réduction de trafic en interne
    - Moins de pression pour l'administrateur