# DNS et lutte anti-spam

**Pierre-Yves Bonnetain**

**B&A Consultants**

**py.bonnetain@ba-cst.com**

# Préambule

- Cette présentation est inspirée de celle de M. Stéphane Bortzmeyer, du NIC France (bortzmeyer@nic.fr), avec son autorisation.
- Version originelle :

  http://www.generic-nic.net/formation/lmap/transparents.pdf

# Quelques rappels

- Le courrier électronique se transmet de MTA en MTA : SMTP, où T = *Transfert*.
- Généralement aucune authentification.
- SMTP est aussi utilisé comme protocole de *soumission* de messages : MUA vers MTA.
- La RFC 2476 vise à « réserver » SMTP pour la communication MTA/MTA, en créant un MSA (Message Submission Agent).

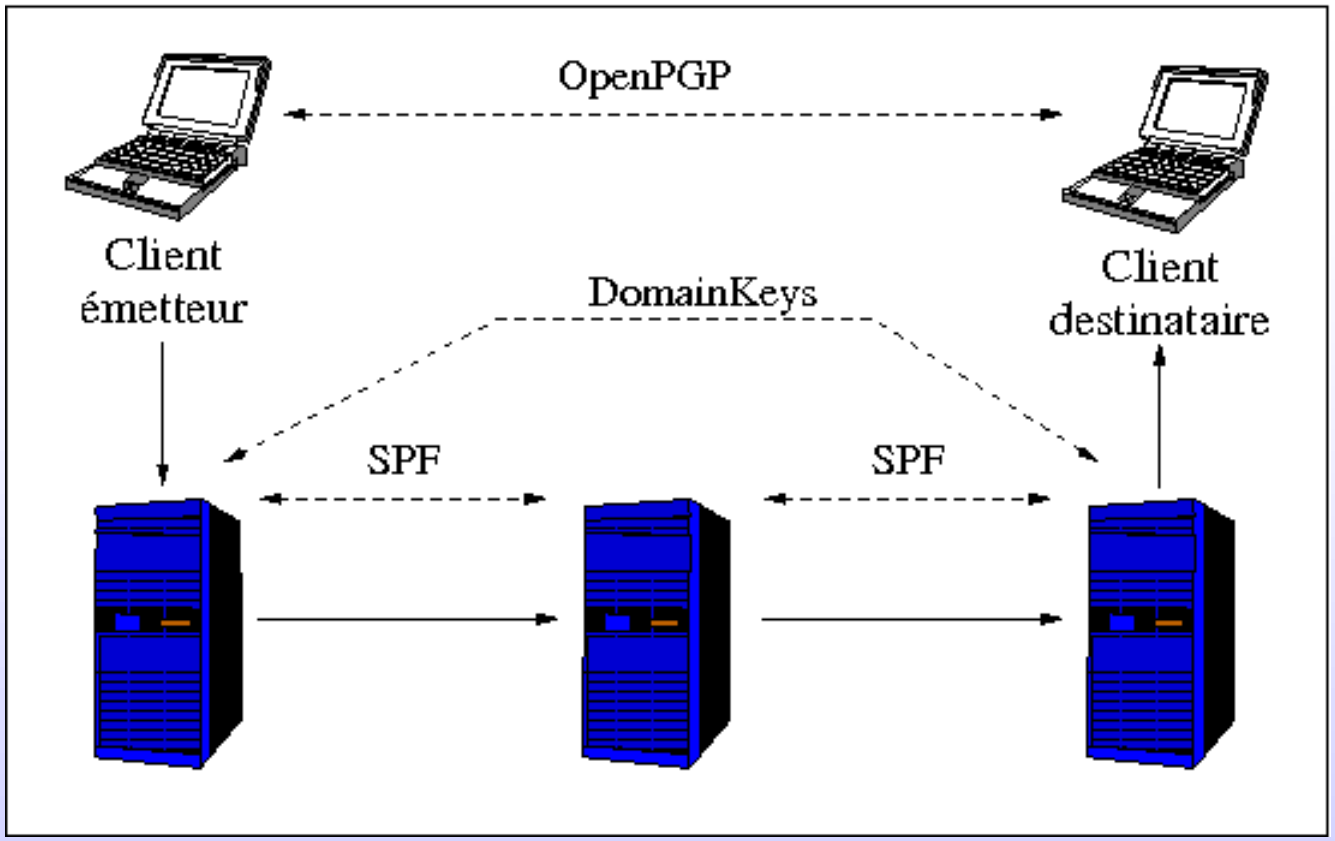
# LMAP

- Lightweight MTA Authentication Protocol
- Principe de base : insérer dans le DNS des enregistrements identifiant les serveurs autorisés à *émettre* pour un certain domaine.
- Le MX de réception fait le contrôle.
- DomainKeys repose sur la même idée (signature numérique, clé publique dans le DNS).

# Authentification émetteur

- On peut envisager des techniques
  - de bout en bout : OpenPGP (RFC 2440) ou DomainKeys.
  - Canal par canal : de type LMAP
- Les techniques de bout en bout sont plus efficaces, mais coûteuses et complexes (certificats, etc.).

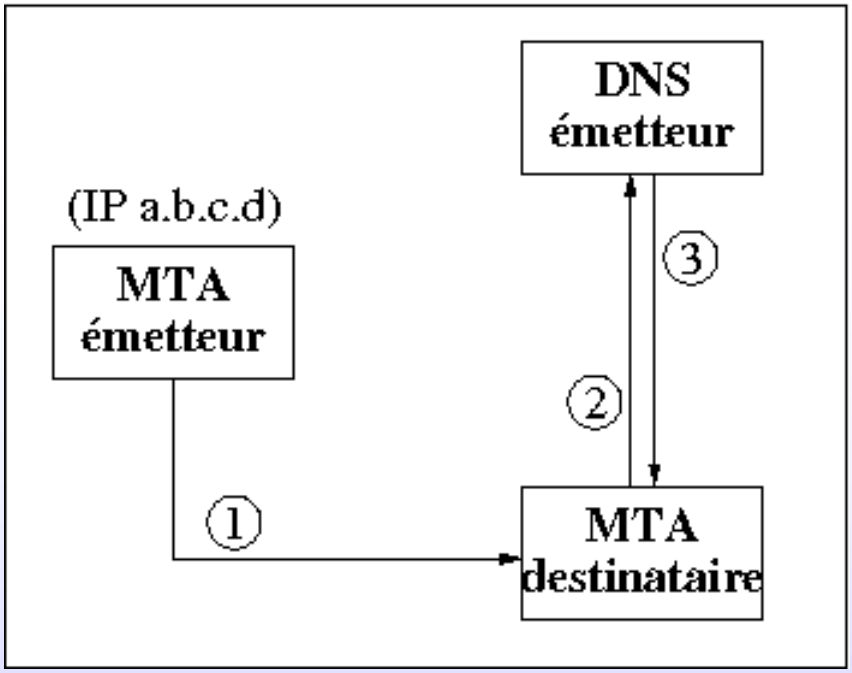
# De bout en bout ou par canal



# Les antécédents

- Paul Vixie, ops.ietf.org/lists/namedroppers/namedroppers.2002/msg00658.html
- Reverse MX, www.danisch.de/work/security/antispam.html (qui ne repose plus sur le DNS).

# Cinématique des échanges




- Le MTA récepteur interroge le DNS
- En fonction des données reçues, il traite ou rejette le message.

# Qui est l'émetteur ?

- LMAP authentifie un domaine (@domaine) et non pas une adresse (untel@domaine).
- Plusieurs manières de « lire » l'émetteur.
- Enveloppe (RFC 2821) MAIL FROM
- En-têtes (RFC 2822)
- PRA (Purported Responsible Address), en-têtes 2822 Resent-From, Sender, From

# Une session typique MTA/MTA

```
Response: 220 YSmtp mta317.mail.scd.yahoo.com
   ESMTP service ready
Command: EHLO relais.ba-cst.com
Response: 250-mta317.mail.scd.yahoo.com
Command: MAIL FROM:<py.bonnetain@ba-cst.com>
Response: 250 sender <py.bonnetain@ba-cst.com> ok
Response: 250 recipient <sargastic@yahoo.fr> ok
Response: 354 go ahead
Message Body
Message Body
Response: 250 ok dirdel
Response: 221 mta317.mail.scd.yahoo.com
```

# Les possibilités

- Comment identifier : RFC2821-MAIL FROM, RFC2822-From:, PRA ?
- Comment établir les autorisations : langage structuré, XML ?
- Comment transporter et obtenir les autorisations : nouveaux enregistrements DNS, TXT, sous-domaine spécial, autre protocole que DNS ?

# Caller-ID : Microsoft

- Identification via PRA (et un brevet).
- Utilise XML, le DNS, et l'enregistrement TXT.
- Utilise un sous-domaine _ep

```
$ dig +short TXT _ep.hotmail.com
"<ep xmlns='http://ms.net/1'
testing='true'><out><m>
<indirect>list1._ep.hotmail.com
</indirect>
<indirect>list2._ep.hotmail.com
</indirect>
<indirect>list3._ep.hotmail.com
</indirect></m></out></ep>"
```

# Sender Policy Framework (SPF)

- Créé et maintenu par Pobox, spf.pobox.com
- Identification via MAIL FROM RFC 2821
- Utilise le DNS, enregistrement TXT, et une syntaxe simple.
- Associé au domaine directement.

```
$ dig +short TXT ba-cst.com
"v=spf1 a:a.mx.ba-cst.com ~all"
$ dig +short TXT univ-tlse1.fr
"v=spf1 mx ip4:193.49.48.253 ~all"
```

# Mise en oeuvre de SPF

- Très facile si on peut éditer son propre fichier de zone.
- Pour les « interfaces conviviales », c'est moins évident...
- Attention aux sous-domaines :
  - Ne pas les oublier s'ils émettent des messages.
  - Bien les « bloquer » sinon (www.domaine.com)

# SPF, DNS et TXT RR

- Taille des enregistrements, et taille maximale des paquets UDP.
- Délai de propagation d'une modification.
- Données « relativement » statiques.
- Révèle l'architecture du relayage de la messagerie.

# SPF et le forwarding

- Problème : le forwarding ne change pas le MAIL FROM.
- SRS (Sender Rewriting scheme) peut être utilisé : http://spf.pobox.com/srspng.html

# Discussion sur le forwarding

- Stuart D. Gathman sur http://archives.listbox.com/spf-discuss@v2.listbox.com/200410/0488.html
- En résumé : si A utilise un forwarder (adr1@domaine1 vers adr2@domaine2)...
- ... il doit le signaler au gestionnaire de domaine2...
- ... qui doit adapter sa configuration.

# Syntaxe SPF

- v=spf1 mécanisme[:valeur] ...
- Mécanismes usuels :
  - a : adresses IP du domaine
  - mx : enregistrements MX
  - ip4 ou ip6 : adresses IPv4 ou IPv6
  - all : Internet

```
$ dig +short TXT freebsd.org
"v=spf1 ip4:216.136.204.119 ~all"
```

- spf.pobox.com/mechanisms.html

# Syntaxe SPF

- Préfixes supplémentaires :
  - + : ajouter cette adresse à la liste (défaut).
  - - : retirer cette adresse à la liste.
  - ? : je ne sais pas.
  - ~ : probablement pas.
- Les deux derniers peuvent correspondre à un système de « points » de type SpamAssassin.

# Exemples

```
$ dig +short TXT nordnet.fr
"v=spf1 mx ptr ip4:194.51.85.0/24
ip4:194.206.126.0/24 ~all"
```

- Peuvent alors envoyer des messages :
  - mx : tous les mx de nordnet.fr,
  - ptr : toutes les machines dont le nom se termine par nordnet.fr.
  - ip4: les deux réseaux 194.51.85.0/24 et 194.206.126.0/24
  - ~all : pour le reste, c'est plus douteux.

# Vérification de la configuration

- Générateur d'enregistrements TXT sur spf.pobox.com/wizard.html.
- Adresse spfenabled@pobox.com (question : quel retour quand SPF correct ou non, ou pour un message illégitime ?).
- spftools.infinitepenguins.net/check.php

# Utilisation de SPF en réception

- Mises en œuvre pour les principaux MTA
- Plusieurs bibliothèques libres.
- Une bibliothèque Perl, Mail::SPF::Query.
- Pour Postfix
  - Postfix Policyd 1.06
  - spf.pobox.com/postfix-policyd.txt (programme Perl)
- Pour sendmail
  - Milter-SPF 1.41
  - spf.pobox.com/sendmail-milter-spf-1.41.pl
- spf.pobox.com/downloads.html

# Configuration Postfix

- Fichier master.cf :

  spf-policy unix ... spawn user=nobody
  argv=/etc/postfix/spf.pl

- Fichier main.cf

  smtpd_recipient_restrictions =

  ...

  check_policy_service unix:private/spf-policy

# Le bilan

- 1527 messages reçus, dont
  - 1280 SPF none : pas d'enregistrement SPF
  - 1 SPF unknown : erreur
  - 216 SPF pass : émetteur validé.
  - 7 SPF fail : émetteur rejeté.
  - 8 SPF neutral : le domaine émetteur veut que l'on ignore son enregistrement SPF
  - 15 SPF softfail : émetteur non validé, mais ?all
- 16% des messages « couverts » par SPF.

# Conclusions

- Intéressant pour éviter la mascarade d'émetteur.
- Facile à activer (DNS) et à utiliser (MTA).
- Les spammeurs peuvent disposer de leurs propres domaines jetables, avec des bons enregistrements SPF.
- Pour la lutte anti-spam, ne suffit pas.
- Une corde supplémentaire, pas un outil terminal.

# Et demain ?

- SenderID (= SPF + Caller-ID) a été rejeté, notamment du fait des brevets et licences Microsoft.
- DomainKeys commence à peine son déploiement.
- RFC expérimentale pour « Classic SPF »
- « Unified SPF », pour appliquer SPF à autre chose que RFC2821-MAIL FROM (notamment au PRA).