

Slide 0

**Les protocoles LMAP : authentifier  
le courrier via le DNS**

**Stéphane Bortzmeyer**

`<bortzmeyer@nic.fr>`

**7 septembre 2004**

Slide 0

Ce document est distribué sous les termes de la  
GNU Free Documentation License <http://www.gnu.org/licenses/licenses.html#FDL>.

Permission is granted to copy, distribute and/or  
modify this document under the terms of the  
GNU Free Documentation License, Version 1.2  
or any later version published by the Free  
Software Foundation ; with no Invariant  
Sections, no Front-Cover Texts, and no  
Back-Cover Texts.

**Slide 1**

**Rappel sur le courrier**

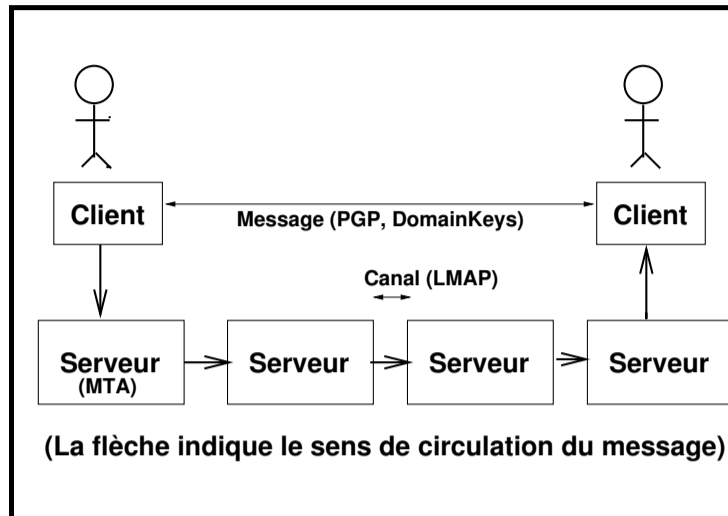
Le courrier est transmis de MTA (Message Transfer Agent) en MTA.

Le protocole principal est SMTP (mais voir RFC 2476).

Typiquement aucune authentification.

RFC 2476 décrit un protocole proche de SMTP pour soumettre le message original. L'idée est de réserver SMTP aux communications MTA-MTA et d'utiliser RFC 2476 pour les communications MUA-MTA.

Slide 2



Certaines techniques authentifient le message : PGP (RFC 2440) ou Domain-Keys, donc couvrent tout le voyage.

D'autres authentifient seulement un canal : c'est le rôle des protocoles LMAP.

Tout le monde est d'accord pour dire qu'authentifier le message est mieux. Mais c'est plus compliqué et coûteux (PKI, par exemple).

D'où l'idée d'une authentification plus faible, celle du canal, qui pourrait approcher les 100 % de déploiement.

**Slide 3**

**Une session typique**

```
S: 220 company.com ESMTP server ready
C: EHLO almater.edu
S: 250-company.com
S: 250 SIZE
C: MAIL FROM:<alice@example.com>
S: 250 <alice@example.com> sender ok
C: RCPT TO:<bob@company.com>
S: 250 <bob@company.com> recipient ok
C: DATA
S: 354 okay, send message
C: Resent-From: bob@almater.edu
C: (message body goes here)
```

**Slide 4**

**Rappel : sécuriser SMTP**

Soumettre seulement : RFC 2476 "Message Submission".

Extensions SMTP pour le relayage sûr : RFC 2554 "SMTP Service Extension for Authentication" et 3207 "SMTP Service Extension for Secure SMTP over Transport Layer Security".

### Tout peut être faux

#### Slide 5

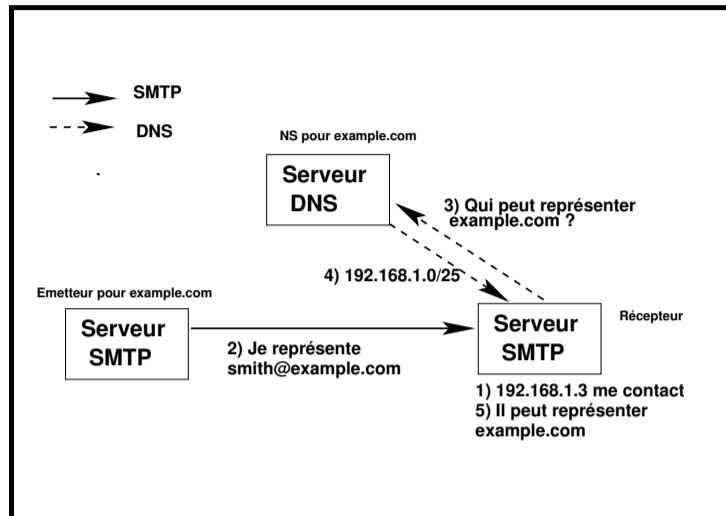
Le principe de LMAP (Lightweight MTA Authentication Protocols) : publier dans le DNS la liste des serveurs SMTP autorisés **pour un domaine**.

Rappelons que, sans LMAP ni PGP, déterminer l'authenticité d'un message nécessite une analyse soignée des en-têtes par un expert. Le but de LMAP est de rendre cette analyse automatique.

Donc, but de LMAP : authentifier le canal SMTP. On en attend :

- Un meilleur fonctionnement des listes blanches
- Une meilleure lutte contre le *phising*
- Une meilleure lutte contre le *spam*

Slide 6



Maintenant, que veut dire “je représente”? D’où vient l’adresse smith@example.com?

### Petit rappel sur les adresses

Enveloppe : RFC 2821 MAIL FROM (ne change pas en cas de *forwarding* (.forward) mais change en cas de *remailing* (procmail)).

En-têtes : RFC 2822

PRA (Purported Responsible Address) extraite des en-têtes 2822 (typiquement Resent-From puis Sender puis From)

Slide 7

L'algorithme PRA tente d'extraire des en-têtes RFC 2822 une adresse unique qui est "responsable pour la dernière introduction dans le système de courrier".

**Slide 8**

### Les choix pour un protocole LMAP

1. identification : que vérifier, 2821 MAIL FROM ou 2822-From : ou PRA
2. authentification : comment le vérifier ?
3. autorisation : quel langage pour exprimer la liste des serveurs autorisés ? XML or not XML ?
4. transport : nouveau type de RR DNS ou bien TXT ? Sous-domaine ?

**Slide 9**

### Les ancêtres

Le document historique de Paul Vixie  
<http://ops.ietf.org/lists/namedroppers/namedroppers.2002/msg00658.html>  
RMX (MX inverse) <http://www.danisch.de/work/security/antispam.html>

Slide 10

### Microsoft : Caller-ID

1. identification : PRA (et breveté)
2. authentification : Session TCP
3. autorisation : XML
4. transport : TXT RR dans 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>
</m></out></ep>"
```

Slide 11

### Le plus déployé : SPF

Sender Policy Framework  
<http://spf.pobox.com/>  
Créé et maintenu par Pobox.

**Slide 12**

**SPF en quatre points**

1. identification : 2821 MAIL FROM (casse le *forwarding*)
2. authentification : Session TCP
3. autorisation : langage texte `v=spf1 mx/25 -all`
4. transport : TXT RR dans le domaine (motivation principale : faciliter le déploiement par tous)

**Slide 13**

**SPF en pratique**

Publier le SPF : trivial si on peut éditer le fichier de zone (piège avec les sous-domaines, toutefois).

Mais tout le monde n'a pas accès au fichier de zone (*provisioning issue*). Problème des interfaces "conviviales".

**Slide 14**

**SPF déployé**

Nombre de déploiements : dans les cinquantes domaines dans “fr” mais en rapide augmentation (et un pourcentage bien plus grand dans “de”). Beaucoup de grands noms.

**Slide 15**

**Vérifier le SPF**

Mises en oeuvre pour tous les MTA. Au moins trois bibliothèques libres.

Exemple avec Postfix et un *policy server* trivial sur la prise *policy*, écrit en Perl avec

Mail : :SPF : :Query :

```
smtpd_recipient_restrictions = ...  
    check_policy_service unix:private/policy, ...
```

## La syntaxe SPF

`v=spf1 mécanisme:[valeur] ...`

Exemple :

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

Mécanismes typiques :

- a : adresses IP du domaine (v4 ou v6)
- mx : enregistrements MX
- ip4 : adresses IPv4
- all : tout l'Internet

Slide 16

“a” désigne les adresses d'un domaine (indiqué en valeur). “ip4” ou “ip6” donnent directement les adresses. Ils sont donc moins souples en cas de re-numérotation mais nécessitent moins de requêtes DNS.

Slide 17

### Préfixes SPF typiques

Devant le mécanisme (+ par défaut) :

- "+" ajouter
- "-" enlever
- "?" ne sais pas
- "~" probablement pas

Slide 18

### Exemples SPF

```
nordnet.fr. IN TXT \  
    "v=spf1 mx ptr ip4:194.206.126.0/24 ~all"
```

Tous les MX de "nordnet.fr", toutes les machines dont le nom se finit en "nordnet.fr", tout 194.206.126.0/24 peuvent envoyer du courrier pour "nordnet.fr". Pour le reste de l'Internet, c'est douteux.

Slide 19

### Résultats SPF à l'AFNIC

Dans le monde réel : encore trop peu d'enregistrements SPF et trop "laxistes" (?a11).

Certains spammeurs se font avoir : "cedex.net" publie du SPF et stoppe donc le *phising*.

Ajouter un test SPF à DNSDoctor ?  
censuré.fr publie un enregistrement SPF invalide...

Slide 20

### Résultats SPF à l'AFNIC, suite

Boîte personnelle : 10 % de "SPF pass", aucun "SPF fail", le reste est neutre.

Boîtes officielles de l'AFNIC (nic@, hostmaster@, etc) : 2 % de "SPF pass", aucun "SPF fail", le reste est neutre.

Sur ma boîte spam : 2 % de "SPF pass" (les spammeurs peuvent mettre du SPF eux-aussi), 1 % de "SPF fail", le reste est neutre.

**Slide 21**

**Le protocole IETF, Sender-ID**

En *Working Group Last Call* depuis le 23 août.

1. identification : PRA (menace de brevet Microsoft) ; 2822 Resent-From puis Sender puis From.
2. authentification : Session TCP
3. autorisation : langage texte, celui de SPF
4. transport : TXT RR dans le domaine puis nouveau type de RR

**Slide 22**

**Techniques non-LMAP**

DomainKeys : authentification du domaine par la cryptographie

OpenPGP, S/MIME : authentification de l'émetteur par la cryptographie

**Slide 23**

### L'avenir

Sender-ID sera t-il déployé ? SPF résistera t-il ?  
Que feront les spammeurs ? Quelle sera  
l'ampleur des dégâts collatéraux lorsque le  
déploiement de LMAP commencera  
sérieusement ?

Sender-ID a été rejeté par Apache, Postfix,  
Courier, Exim, la FSF, etc en raison du brevet  
Microsoft. Le débat a posé la question de la  
politique IPR de l'IETF.

**Slide 24**

### L'avenir unifié

“Unified SPF” essaie de reprendre les  
enregistrements SPF mais en les appliquant à  
d'autres adresses que le 2821 MAIL FROM  
(par exemple au PRA) : un sur-ensemble qui  
mettra tout le monde d'accord ?