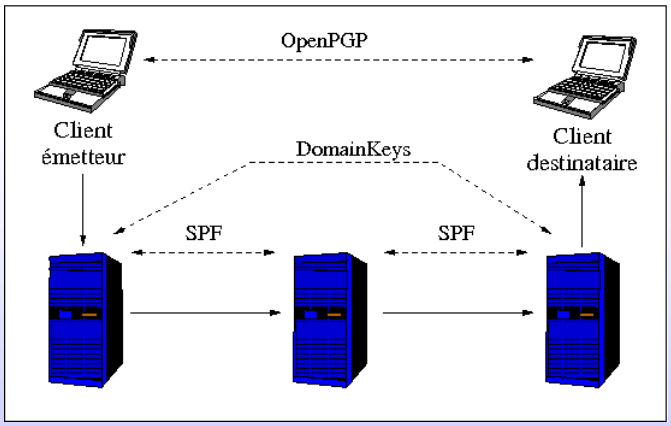
SPF, DomainKeys, DKIM

Pierre-Yves Bonnetain
B&A Consultants
py.bonnetain@ba-cst.com

Authentification des messages

- On peut envisager des techniques
  - de bout en bout : OpenPGP ou DomainKeys.
  - Canal par canal : de type LMAP/SPF
- Les techniques de bout en bout sont plus précises.
- Mais plus complexes :
  - clés de chiffrement,
  - modules de signature/vérification des signatures,
  - etc...

De bout en bout ou par canal



LMAP/Sender Policy Framework

- Lightweight MTA Authentication Protocol
- Principe de base : insérer dans le DNS des informations identifiant les serveurs autorisés à *émettre* pour un certain domaine.
- Le MX de réception fait le contrôle.
- Contrôles reposant sur l'adresse IP du MTA opposé.

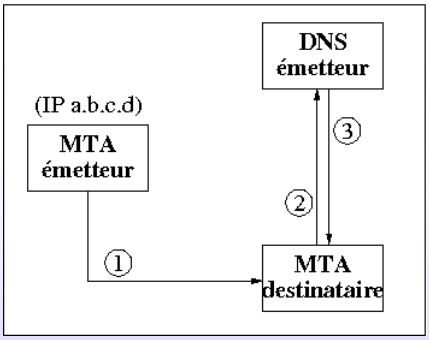
DomainKeys, DKIM

- DomainKeys repose sur une signature cryptographique automatique des messages.
- Le MX émetteur dispose de la clé privée du domaine.
- La clé publique est diffusée via le DNS (ou d'autres canaux, à venir).

Quelques références

- SPF : www.openspf.org
- DomainKeys et DomainKeys Identified Mail
  - antispam.yahoo.com/domainkeys
  - www3.ietf.org/proceedings/04aug/slides/mass-1.pdf
  - domainkeys.sourceforge.net
  - www.dkim.org

Cinématique des échanges



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

Sender Policy Framework (SPF)

- Créé par Pobox (www.pobox.com).
- spf.pobox.com renvoie sur www.openspf.org
- Identification via MAIL FROM (RFC 2821)
- Utilise le DNS, enregistrement TXT.
- 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 ip4:193.49.48.247
~all"
```

SPF et le forwarding

- Problème : le forwarding ne change pas le MAIL FROM.
- SRS (Sender Rewriting scheme) peut être utilisé : http://www.openspf.com/srspng.html
- C'est un peu complexe...

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.

DomainKeys

- DK signe un ensemble d'en-têtes ainsi que le corps du message.
- Il « suffit » de disposer de la clé privée d'un domaine.
- Ne révèle pas l'architecture de la messagerie sortante.
- Permet de déléguer des signatures.
- Permet de définir des « sous-domaines » de signature.

DK et DKIM

- Clés publiques dans le sous-domaine _domainkey.
- Actuellement TXT RR, nouvelle ressource en cours de définition.
- Utilise des « sélecteurs » dans le sous-domaine _domainkey.
- Exemple : sélecteur beta, domaine gmail.com.
  - `DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=beta; d=gmail.com; h=received:message-id:date:from:sender:to:subject:mime-version:content-type; b=Vk5RTnKo+[...]=`

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"
```

- www.openspf.org/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.
- Générateur d'enregistrements TXT sur www.openspf.org/wizard.html.

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.

DK, déclaration de politique

- Pas de protocole pour qu'un domaine
  - Indique sa politique de signature.
  - Dise comment traiter les messages mal signés.
- Situation temporaire (promise à durer) tant qu'il n'existe pas de standard.
- Dans _domainkey.domain.tld :
  - t=y (test de DK; optionnel)
  - o=[-|~] (tous messages sortants signés/certains seulement; défaut ~)

Exemples de politiques

```
_domainkey.yahoo.com    text =
        "t=y; o=~; n=http://antispam.yahoo.com/domainkeys"
```

```
Réponse ne faisant pas autorité :
_domainkey.22c.net      text =
        "r=dshattuck@mediaplex.com;"
```

```
Réponse ne faisant pas autorité :
_domainkey.dell.com     text =
        "t=y; o=~"
```

La majorité des sites utilisant DomainKeys se présentent comme « testant DK ».

Syntaxe DomainKeys (DNS)

- v=DKIM1 (version; optionnel)
- t=y (indicateurs booléens; seul y est valide, signifiant que DK est en tests au site émetteur; optionnel)
- k=rsa (algorithme pour la signature; optionnel, RSA par défaut)
- p=... (clé publique)

Exemples

- beta._domainkey.gmail.com
  - t=y; k=rsa; p=MIGfM...
- s1024._domainkey.yahoo.fr
  - k=rsa; t=y; p=MIGfM...; n=A 1024 bit key;
- Attention : sous-domaine _domainkey (sans S terminal)

```
pyb@nihao:~
[pyb@nihao ~]$ dig +short -t TXT dk20050327._domainkey.mindspring.com
"g=\; k=rsa\; t=y\; p=MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxALigv1kAvfPxsUFY5vobiVUevC
AK7qzzBDTz1+iYqOXPFxIkMQFhQuwh6GNpVPRROwIDAQAB"
[pyb@nihao ~]$
```


En-tête DK, validation

- Insertion d'un en-tête DomainKey-Signature dans les messages émis.

```
Received: by nz-out-0102.google.com with SMTP id x7so543893nzc
        for <infos@ba-cst.net>; Mon, 29 May 2006 00:40:17 -0700 (PDT)
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
        s=beta; d=gmail.com;
        h=received:message-id:date:from:to:subject:mime-version:content-typ
        b=hIotOjYOM37JEqK9vWDahuY+3OZ6lq5zZuAgohXDtcuAQkYSQhEINHZEKoOe+Gg/O
Received: by 10.65.252.18 with SMTP id e18mr770970qbs;
        Mon, 29 May 2006 00:40:17 -0700 (PDT)
Received: by 10.65.81.15 with HTTP; Mon, 29 May 2006 00:40:17 -0700 (PDT)
```

- Quelques sites (Gmail, Yahoo) affichent la bonne validation (DK et SPF pour GMail)

En-tête DomainKey-Signature

- a=algorithme cryptographique (défaut rsa-sha1)
- q=récupération de la clé publique (défaut dns)
- c=algorithme de canonisation des données à signer. Obligatoire. simple|nofws
- s=sélecteur utilisé. Obligatoire.
- d=domaine du signataire. Obligatoire.
- b=signature du message. Obligatoire.
- h=liste des en-têtes utilisés. Si présent, doit indiquer l'en-tête servant à définir le domaine émetteur (From:, Sender:, etc.)

Traitement des en-têtes

- Le champ (optionnel) h donne la liste des en-têtes à prendre en considération, dans l'ordre indiqué.
- Ce sont des en-têtes placés APRES l'en-tête DomainKey-Signature.
- Tous les exemplaires d'un en-tête dupliqué (Received:) doivent être pris en compte.
- Permet de s'affranchir des en-têtes ajoutés ensuite par les systèmes de messagerie en aval de l'émetteur.

Différences DK/DKIM

- DKIM est une évolution de DomainKeys
- Le signataire peut différer de l'auteur ou de l'émetteur
  - Signature par des tierces parties
  - Fournisseur de messagerie, indépendant du domaine de l'émetteur.
- Le champ DKIM est autosigné.
- La liste des en-têtes signés n'est plus optionnelle.
- La signature peut inclure un délai de validité au-delà de laquelle elle expire (t=, x=)

Outils SPF

- Versions pour les principaux MTA
- Plusieurs bibliothèques libres.
- Intégré dans SpamAssassin.
- Une bibliothèque Perl, Mail::SPF::Query.
- Postfix Policyd 1.07
  - www.openspf.org/source/*checkout*/mail-spf-query-perl/trunk/examples/postfix-policyd-spf
- Milter-SPF 1.42
  - srs-socketmap.info/spf/sendmail-milter-spf.pl
- openspf.org/downloads.html

Outils DomainKeys

- domainkeys.sourceforge.net/
- Dkfilter (postfix) jason.long.name/dkfilter
- Domainkeys-milter (sendmail) sourceforge.net/project/showfiles.php?group_id=110311&package_id=119545
- Qmail-dk (patch pour Qmail)
- ... et d'autres, voir sur domainkeys.sourceforge.net

Outils DKIM

- Dkim-milter (sendmail) sourceforge.net/projects/dkim-milter
- Dkimproxy (postfix) jason.long.name/dkimproxy
- Bibliothèque libdkim http://libdkim.sourceforge.net

Bilan SPF/SpamAssassin

- 9819 messages avec infos SPF sur 97943 :
  - 9607 SPF pass (9,81% des messages, 97,84% des messages « avec SPF ») : émetteur valide (49 classés en spam ensuite : 0,5 %)
  - 73 SPF fail (0,74%) : émetteur rejeté.
  - 139 SPF softfail (1,42%): émetteur non validé, mais ?all.
- 10% des messages « couverts » par SPF.

Bilan DK/SpamAssassin

- Sur 37899 messages, 3927 concernés par DK :
  - 2744 (7,24%) avec en-tête Domainkey-Signature
    - Dont 341 validés (12,43% des messages avec l'en-tête, 0,9% des messages reçus)
    - Sur les 341 validés, 3 classés en spam ensuite (par DCC).
  - 1183 (3,12%) pour sites « tests DK », sans signature dans les en-têtes.
- 10,4 % des messages « couverts » par DK

Conclusions

- Intéressant pour éviter la mascarade d'émetteur.
- SPF facile à activer (DNS) et à utiliser.
- DK/DKIM un peu plus délicat à utiliser (modules supplémentaires).
- Les spammeurs peuvent disposer de leurs propres domaines jetables, avec des bons enregistrements SPF ou signatures DK.
- Pour la lutte anti-spam, ne suffit pas.
- Une corde supplémentaire, pas un outil terminal.