1. Présentation de SPF

Support de la présentation :

- HTML : http://www.ba-cst.com/presentations/Lmap/index.html
- PDF : http://www.ba-cst.com/presentations/Lmap/Lmap.pdf

SPF (Sender Policy Framework) correspond à l'utilisation de requêtes DNS afin de permettre à un serveur de messagerie, sur réception d'un message, de « valider » l'adresse de l'émetteur. L'idée sous-jacente est d'authentifier, autant que possible, l'émetteur d'un message afin d'éviter les spams. Outre SPF, SenderId et DomainKeys visent à résoudre le même problème.

Le principe est d'interroger le serveur DNS du domaine de l'émetteur du message, pour lui demander le champ TXT associé au domaine. Dans le cadre de SPF, ce champ contient la liste des serveurs autorisés à émettre un message pour le domaine en question. De cette manière, le serveur destinataire peut s'assurer que le message a bien été émis par un serveur « autorisé à émettre » par rapport au domaine de l'expéditeur.

L'une des questions qui se pose est de déterminer l'émetteur. Est-ce celui de l'enveloppe du message (mail from au sens SMTP) ou du contenu (from:) ?

SPF est facile à mettre en place pour un site émetteur. Il suffit d'éditer l'enregistrement TXT associé au domaine en question. La syntaxe à utiliser n'est pas complexe.

Pour un site voulant vérifier qu'un message reçu est bien émis par un serveur habilité pour cela, il faut coupler SPF au relais de messagerie. Le couplage se fait soit directement, au niveau du MTA, soit en activant la vérification SPF dans un outil comme SpamAssassin.

SPF pose quelques difficultés, notamment pour ce qui est réacheminement de messages. Si un courrier va de *dupont@domaine1.tld* vers *dupond@domaine2.tld*, le MX de *domaine2.tld* peut vérifier qu'il reçoit bien ce message depuis un serveur d'émission valide pour *domaine1.tld*.

Mais si l'adresse *dupond@domaine2.tld* est réacheminée vers *martin@domaine3.tld*, le MX de *domaine3.tld* ne pourra pas faire ce contrôle (ou, plus exactement, le contrôle échjouera). En effet, c'est un serveur de *domaine2.tld* qui enverra le message à l'un des MX de *domaine3.tld*, et ce serveur d'émission/réacheminement n'a aucune raison d'être identifié comme émetteur légitime pour *domaine1.tld*.

A l'usage, on constate que SPF n'est pas un bon test définitif (accepter/refuser un message uniquement sur la base des informations SPF) mais un bon test de type bayesien (paramètre supplémentaire pour juger de la nature pourriel/légitime d'un message).

Quels sont les problèmes liés à la longueur du champ TXT ?

Le basculement de UDP vers TCP n'est pas toujours possible (filtres IP), ce qui nécessite de prendre quelques précautions. Ily a plusieurs possibilités.

- SPF permet de construire des enregistrement modulaires (voir celui de hotmail.com par exemple), un enregistrement peut alors rester inférieur à 512 octets, et transiter via UDP.
- La RFC 2671 (EDNS0), mise en œuvre par BIND, permet d'éviter l'utilisation de TCP.

Il est à noter que l'AFNIC considère qu'un site qui filtre TCP/53 n'est pas conforme. De tels sites ne peuvent obtenir un domaine en .fr, le contrôle via zonecheck étant alors négatif.

Quelle est la charge DNS supplémentaire provoquée par SPF ?

Il y a « mécaniquement » une augmentation de la charge, mais elle reste faible voire négligeable. Si l'on craint une trop forte sollicitation du DNS, on peut toujours (une fois les données SPF correctement validées) d'augmenter le TTL de cet enregistrement.

Quels sont les fournisseurs d'accès ayant activé SPF ?

Les plus visibles sont AOL (spf 1.0 et 2.0) et hotmail (spf 1.0). En France, Nordnet (nordnet.fr) et ClaraNet (fr.clara.net). Il y en a probablement d'autres.

Peut-on mettre un champ TXT par machine ?

Oui.

Quelle est la proportion d'utilisateurs du SPF ?

A l'UT1, 36% des messages reçus correspondent à des domaines ayant un enregistrement TXT. Sur d'autres sites, le pourcentage varie entre 10 et 30%.

2. Protection anti-virale en profondeur

Support de la présentation :

- PDF :
  http://www.ossir.org/resist/supports/cr/20041129/ProtectionViraleEnProfondeur.pdf

Concernant la protection contre les virus, il est malheureux de constater que :

- Les auteurs de virus sont de véritables professionnels.
- Les virus sont souvent « optimisés » pour se propager le plus vite possible, en interne (réseau local) ou en externe.
- Lors de l'apparition d'un nouveau virus, il faut entre 2 et 4 heures pour que les systèmes anti-viraux commencent à les détecter (analyse, création d'une nouvelle signature, diffusion).

La protection basée sur les anti-virus se révèle nécessaire, mais n'est plus vraiment suffisante, ne serait-ce que pour surmonter une infection en attendant la mise à jour de l'éditeur. Une attitude plus active est souvent nécessaire.

L'Université de Toulouse 1 a adopté une stratégie visant à détecter les comportements de « type viral », afin d'isoler partiellement ces systèmes et de limiter la propagation d'une infection. Cette stratégie de détection repose sur

- un point de collecte des alertes, qui sont remontées par différents outils (garde-barrière personnel, routeurs filtrants, garde-barrière de l'Université, etc.), et
- l'information de l'utilisateur du poste infecté (redirection de sa navigation Web vers une page dédiée pour l'aider à se décontaminer).

Le point de collecte examine toutes les alertes reçues. Sur le franchissement de certains seuils (par exemple, pour un même poste, plus de 10 tentatives d'émission directe de messages électroniques, sans passer par la passerelle officielle, sur 10000 lignes de journal), le poste concerné est mis en quarantaine. Cette quarantaine vise à limiter la propagation d'un virus non encore détecté par les outils anti-viraux.

Cette stratégie permet aujourd'hui à l'UT1 de détecter très rapidement tout nouveau poste infecté, de réagir en moins de 30 minutes sur l'apparition d'un virus inconnu au sein du réseau et, dans un tiers des cas, de faire exécuter la décontamination par l'utilisateur du poste.

L'essentiel des difficultés rencontrées pour la mise en place de cette stratégie concerne la modification dynamique des règles de routage/filtrage afin de « bloquer » un poste. Il faut absolument éviter de perdre toutes les connexions en cours au travers du ou des équipements qui sont reconfigurés (filtrage dynamique, suivi des connexions, etc.) : les autres utilisateurs ne doivent pas être perturbés.