RFC 5016 : Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices Protocol

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 novembre 2007. Dernière mise à jour le 24 août 2009

Date de publication du RFC : Octobre 2007

https://www.bortzmeyer.org/5016.html

Le protocole DKIM de signature des courriers électroniques a une limite. Tant que tout le monde ne signe pas, on ne peut pas savoir si l'absence de signature est volontaire ou bien est la conséquence d'une fraude. Le protocole SSP ("*Signing Practices Protocol*") doit permettre de résoudre ce problème.

DKIM, normalisé dans le RFC 6376 [1], normalise un mécanisme pour insérer des signatures cryptographiques dans un courrier électronique, de façon à en prouver l'authenticité. Mais le déploiement de DKIM ne sera pas instantané et n'atteindra peut-être jamais 100 % des serveurs de messagerie. Si un message arrive sans signature, est-ce normal car ce domaine ne signe pas, ou bien est-ce une fraude ? Impossible de le savoir sans connaitre les pratiques de signature du domaine. Par exemple `cisco.com` signe tous ses messages. Mais on ne peut pas connaitre les pratiques de tous les domaines de l'Internet. Il faut donc un protocole pour récupérer cette information, SSP, dont ce RFC donne le cahier des charges.

Le principe de SSP est de fournir un moyen permettant à un MTA de décider, lorsque le message n'est pas signé, si cela est suspect ou non. Si SSP indique que `example.net` signe toujours et qu'un message prétendant venir de `dupont@example.net` n'est pas signé, le récepteur pourra donc légitimement le traiter avec une extrême suspicion.

La section 3 du RFC donne divers scénarios d'usage, et la section 4 se penche sur les problèmes de déploiement, un problème difficile pour toutes les nouvelles technologies. Ainsi, la section 4.2 rappelle que le gérant d'un domaine peut avoir envie de couvrir également les sous-domaines (autrement, le méchant qui veut faire croire que son domaine est `example.net` n'aurait qu'à envoyer depuis `staff.example.net`), la section 4.5 insiste sur les questions de performance, etc..

La section 5 attaque les exigences proprement dites. Je ne vais pas les énumérer ici, mais seulement donner quelques exemples :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6376.txt`

— 5.1 (4) reprend le scénario d'une attaque sur un sous-domaine et demande que SSP permette de couvrir les sous-domaines (on note que cela permettrait au gérant de `.com` de définir une politique pour `example.com`...).
— 5.2 (3) exige que la charge entrainée par les requêtes SSP soit bornée (SPF, normalisé dans le RFC 4408, avait été critiqué car son langage, très puissant, permettait d'exprimer des politiques complètes qui auraient pu mener à une avalanche de requêtes DNS à chaque message reçu).
— 5.3 (5) veut que la syntaxe des messages soit compréhensible par un humain et dit, par exemple, que `p=unknown` est préférable à `p=?` (là encore, SPF est sans doute visé, ses enregistrements étant parfois cryptiques).
— 5.3 (9) exige que l'appel à SSP soit facultatif, si la signature DKIM est présente et correcte.

SSP a finalement été spécifié dans le RFC 5617, qui utilise le DNS pour récupérer des politiques ressemblant, pour un domaine qui signe tout et garantit que ces signatures ne sont pas invalidés en cours de route, à `dkim=discardable`.