

L'impact de la lutte contre le SPAM et les virus sur les architectures de messagerie.

Serge Aumont
Comité Réseau des Universités

Claude Gross
Unité Réseau du CNRS

Mots clefs

Bayésien, greylist, DKIM, SPF, SMTP/AUTH, Spam, Virus

Résumé

L'évolution du phénomène du spam dans son ampleur et dans sa nature ne nous permet plus aujourd'hui de se contenter de le supporter simplement comme une gêne. Les buts poursuivis par certains spammeurs font courir un risque sérieux à nos systèmes d'informations. Cet article fait le point sur les méthodes techniques de lutte disponibles aujourd'hui en essayant de dégager une typologie. Il propose une approche pour leur intégration dans une architecture de messagerie dans le but de contrer le plus efficacement possible cette menace.

L'article distingue les flux entrant et sortant du domaine. Il explique pourquoi le traitement anti-spam/anti-virus du flux sortant ne doit pas être négligé. Il distingue les techniques binaires qui aboutissent à un rejet ou non des messages de celles qui donnent un résultat insuffisant pour prendre le risque d'un rejet mais, qui corrélées entres elles, permettent cette prise de décision. Un accent particulier est porté sur les nouvelles techniques d'authentification : SPF (vérification de la provenance des messages) et DKIM (signature cryptographique) parce que leur impact sur l'architecture de messagerie est particulièrement importante.

L'efficacité des techniques de lutte contre le spam a tendance à diminuer parce que les spammeurs les contournent. Aussi faut-il périodiquement reconsidérer les armes de lutte employées. Les changements peuvent être périlleux. C'est pourquoi il est important de définir une architecture modulaire du service de messagerie permettant d'intégrer rapidement de nouvelles techniques.