RFC 4686 : Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 octobre 2006

Date de publication du RFC : Septembre 2006

https://www.bortzmeyer.org/4686.html

Le courrier électronique n'est pas sûr, on le sait bien. Notamment, il ne fournit pas de moyen d'authentifier l'émetteur et il est trivial d'envoyer un message prétendant venir de Nicolas.Sarkozy@poulaga.fr. Une des techniques prétendant traiter ce problème est DKIM et notre RFC décrit les risques auxquels répond DKIM et les menaces contre DKIM.

Précisons tout de suite que DKIM, contrairement à des techniques comme PGP ne vise nullement à la confidentialité des messages mais uniquement à leur authentification. DKIM, normalisé dans le RFC 6376 [1], répond donc aux menaces d'**usurpation** d'une adresse. Le RFC commence par analyser les méchants : ce qu'ils peuvent faire (du "*script kiddie*" au professionnel entrainé), ce dont ils disposent (les algorithmes, par exemple, puisque la norme DKIM est disponible publiquement), ce qu'ils veulent (usurper une identité, bien sûr mais peut-être aussi réaliser une DoS en empêchant des vérifications).

L'essentiel du RFC, sa section 4, est ensuite consacrée à l'examen détaillé de toutes les attaques possibles, du vol de la clé privée à l'exploitation de limites des MUA qui n'afficheraient pas clairement le contenu qui est signé et ce qui ne l'est pas (DKIM permet de ne signer qu'une partie d'un message) ou bien qui afficheraient les parties non-vérifiées d'une adresse au même titre que les parties vérifiées (par exemple, dans l'adresse Ségolène Royal <plaisantin@hotmail.com>, seule l'adresse plaisantin@hotmail.com peut être vérifiée par DKIM, pas le nom affiché).

Beaucoup des attaques décrites ici ne sont pas spécifiques à DKIM, ni même à la cryptographie et on ne peut donc que rappeler les principes de base de la sécurité informatique, notamment le fait que le maillon faible est en général entre la chaise et le clavier...

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