

Authentifier et autoriser, deux choses différentes

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 Février 2007

<http://www.bortzmeyer.org/authentifier-et-autoriser.html>

Je vois déjà apparaitre des articles sur OpenID qui expliquent doctement que cette technologie n'arrêtera pas le spam dans les commentaires sur les blogs car les méchants pourront eux aussi avoir un identifiant OpenID. Pourquoi cette affirmation est-elle stupide ?

J'avais déjà entendu ce genre d'arguments contre SPF (décrit dans le RFC 4408¹) et, d'ailleurs, contre la plupart des techniques d'authentification. Il est tout aussi faux à chaque fois.

Il y a une confusion fréquente, chez les personnes ne connaissant pas la sécurité informatique, entre l'authentification et l'autorisation. Prenons l'exemple d'une personne, moi, capable de s'authentifier, et qui veut pénétrer dans le bureau du président de la République, à l'Élysée. Grâce à ma carte d'identité, je peux prouver que je suis bien Stéphane Bortzmeyer. Si le garde à l'entrée est suffisamment méfiant, ou bien si ses consignes le lui imposent, il peut me demander une deuxième pièce d'identité, me faire passer un examen biométrique, etc, il arrivera toujours à la même conclusion : je suis bien celui que je prétends être. Mais aurais-je l'occasion de rentrer dans le bureau qui est mon objectif ? Probablement pas. Je suis **authentifié** mais pas **autorisé**.

Donc, bien sûr que les spammeurs auront des identifiants OpenID et des enregistrements SPF, de même que des délinquants et des criminels ont une carte d'identité. Il ne faut pas demander à ces techniques d'**authentification** plus que ce qu'elles peuvent donner : elles authentifient, il faut un autre système pour **autoriser** (ou non).

Ces systèmes ne font pas l'objet de cet article. Ils peuvent être fondés sur des listes maintenues localement (je suppose que la liste des personnes travaillant à l'Élysée est gérée ainsi) ou sur des systèmes d'accréditation ou de réputation distribués comme expliqués dans l'article de Phillip J. Windley, "*A Framework for Building Reputation Systems*" <http://www.windley.com/essays/2006/dim2006/framework_for_building_reputation_systems> (<<http://jyte.com/>> est une amusante expérience bâtie sur OpenID à ce sujet) mais ils ont tous en commun de supposer que l'authentification soit fiable. L'autorisation et l'authentification ne servent pas à grand'chose séparément. C'est la combinaison qui les rend intéressantes.

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc4408.txt>