Comment on traduit ≪ nonce ≫ ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 juillet 2012

http://www.bortzmeyer.org/nonce.html

Comme mes fidèles lecteurs (et lectrices) ont l'air d'apprécier les questions de traduction, le problème du jour, motivé par la publication un de ces jours des RFC sur ILNP, est ≪ quelle est la bonne traduction de l'anglais "*nonce*" ? ≫.

Rien à voir avec celui du pape. En informatique, et plus spécialement dans les protocoles réseaux, un "*nonce*" est un nombre imprévisible (de préférence aléatoire), choisi par un des participants à la communication et transmis à l'autre. Ledit autre pourra prouver qu'il est bien toujours le même en produisant ce "*nonce*". Un éventuel attaquant, ne pouvant pas connaître (ou deviner) ce "*nonce*", ne pourra pas usurper l'identité d'une des parties à la communication. Par exemple, les "*Query ID*" du DNS (RFC 5452[1]) ou les ISN (numéros de séquence initiaux) de TCP (RFC 5961) sont des "*nonces*". (Plusieurs lecteurs érudits et attentifs m'ont fait remarquer que ma description était quand même très simplifiée. J'assume.)

Les experts en sécurité auront noté que le "*nonce*" ne protège que contre un attaquant incapable d'écouter la communication. Autrement, si l'attaquant est situé sur le chemin et espionne, le "*nonce*" ne sert à rien puisque ledit attaquant le connait.

Le "*nonce*" n'est donc pas de la cryptographie et il est curieux que les Wikipédia francophones et anglophones le décrivent sous l'appellation de ≪ Nonce cryptographique ≫.

Bon, mais quel terme utiliser en français ? En anglais, ≪ "*nonce*" ≫ veut dire ≪ mot à usage unique <http://en.wiktionary.org/wiki/nonce> ≫. En japonais, on dit simplement "*nonsu*", tiré de l'anglais. On m'a cité les traductions suivantes possibles :

— Valeur de circonstance (correct mais long) voire Nom occasionnel à utilisation limitée ou Nombre à usage unique
— Hapax (traduire de l'anglais par du grec... mais respecte l'origine littéraire du terme anglais)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5452.txt

— Numnique (jolie idée de Steve Schnepp <https://mobile.twitter.com/steve_schnepp> autour de l'idée de « nombre unique ») ou Munique (« mot unique », idée de grommeleur <http://seenthis.net/people/grommeleur>) ou encore Monique (« mot unique », idée de Steve Schnepp <http://twitter.com/steve_schnepp>)
— Mohasard (« mot choisi au hasard »)
— Numéro jetable (idée de Ludovic Rousseau, pour faire passer l'idée que le numéro devient inutile, voir dangereux, une fois qu'il a été utilisé, mais qui ne convoie pas l'idée d'imprévisibilité)
— Défi (on le trouve dans certains articles de Wikipédia <http://fr.wikipedia.org/wiki/Authentification_forte#Authentifieurs_fond.C3.A9_sur_un_m.C3.A9canisme_de_.C2.AB_d.C3.A9fi_r.C3.A9ponse_.C2.BB>)

Qu'en dites-vous ?

Merci entre autre à Jean Rebiffé pour des tas de remarques pertinentes.