Les quatorze qui soi-disant contrôlent tout l'Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 août 2014

https://www.bortzmeyer.org/les-quatorze-qui-controlent-tout.html

---

Hier, le magazine GQ a cru bon de publier un article <http://www.gqmagazine.fr/pop-culture/gq-enquete/articles/qui-detient-vraiment-les-cles-dinternet-/15382> intitulé « Qui détient (vraiment) les clés d[Caractère Unicode non montré [1]]Internet ? » et qui contient tellement d'erreurs, d'exagérations, et de sensationnalisme que c'était un exercice intéressant que de tenter de les lister toutes, de rectifier la vérité de manière (je l'espère) compréhensible par des gens qui ne sont pas des experts de l'infrastructure Internet, et d'en profiter pour regarder comment travaillent les médias auxquels tant de gens font confiance pour s'informer.

D'abord, il faut noter qu'il n'y a aucun travail d'enquête : cet article et d'autres qui l'ont précédé en français (comme celui de Paris-Match <http://www.parismatch.com/Actu/Environnement-et-sciences/Ils-detiennent-les-cles-du-reseau-564381>) sont juste de mauvaises traductions et adaptations d'un article du Guardian <http://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web>, qui était également pas mal sensationnaliste mais qui reposait au moins sur un reportage réel. Chaque adaptation successive de cet article a dégradé un peu plus le contenu. Mais, que voulez-vous, produire du contenu de qualité coûte cher, et adapter des articles déjà faits est plus rapide. Pour faire croire que le contenu est original, l'article doit prétendre qu'il va révéler « un des secrets les mieux gardés » alors que, on l'a vu, ce système a déjà été décrit dans plusieurs journaux.

Maintenant, reprenons l'article de GQ. Il use et abuse de termes sensationnels (« L[Caractère Unicode non montré]histoire est digne d[Caractère Unicode non montré]un film de science-fiction. ») pour faire du spectacle à partir d'une réalité nettement plus austère, qui n'intéresse normalement que les ingénieurs réseau. Résumé simplement, il s'agit de la technologie DNSSEC, un mécanisme technique et organisationnel qui permet de sécuriser une partie importante de l'infrastructure de l'Internet, le système des noms de domaine. Sans DNSSEC, il est relativement facile à un craqueur de subvertir ce système en redirigeant un nom (mettons `bortzmeyer.org` qui sert au courrier que je reçois) ailleurs que ce que voulait le titulaire du nom. Il est amusant que l'article de GQ ne mentionne pas une seule fois ce sigle DNSSEC. Une caractéristique importante de DNSSEC est qu'il est **optionnel** : aujourd'hui,

1. Car trop difficile à faire afficher par LaTeX

seule une petite minorité des noms (`bortzmeyer.org` en fait partie) est protégée par DNSSEC et seule une minorité des utilisateurs se servent de serveurs de noms qui vérifient les signatures que DNSSEC appose. Il est donc ridicule de présenter ce système comme étant **la** sécurité de l'Internet (« le cœur de la sécurité du Net »). Il existe d'autres systèmes de sécurité qui jouent un rôle bien plus important pour l'instant.

Ce n'est pas trop glamour, bien sûr, et donc un certain nombre de personnes ont choisi de gonfler les choses, en menant une politique de communication personnelle active. On l'a vu, produire des articles de qualité coûte cher. Alors que les journalistes sont bombardés de contenus tout prêts, déversés sur eux par des entreprises ou des personnes qui veulent se mettre en avant. Il suffit de reprendre leurs discours, sans contre-enquête, sans nuance critique, et hop, on a une jolie histoire. Sur Internet comme ailleurs, ceux qui communiquent le plus ne sont pas forcément ceux qui font le travail (de « plombiers »)...

Bon, on va être indulgent, on va dire que ces abus sensationnalistes sont un choix de récit, que cela n'affecte pas le fond de l'article.

Mais c'est qu'il y a plein d'erreurs dans l'article. Citons-les dans l'ordre. D'abord, il y a une confusion entre l'Internet et le Web (les deux articles de Wikipédia sur ces deux technologies expliquent bien la différence). Des phrases comme « [une] simple clé qui permet de sécuriser tout le web » sont donc fausses : DNSSEC n'est pas spécifique au Web.

Ensuite, l'article parle d'une « une clé centrale de chiffrement » alors que DNSSEC ne fait pas de chiffrement! Le chiffrement sert à garantir la confidentialité des communications mais ce n'est pas le rôle de DNSSEC. Son rôle est d'assurer l'authenticité des données, via un mécanisme de signature.

Passons sur « des "*data centers*" aussi sécurisés qu[Caractère Unicode non montré]une centrale nucléaire ». Si c'était vrai, les riverains de Fessenheim pourraient s'inquiéter...

Plus embêtant, « Ce que contrôle cette clé centrale est le "serveur-racine" ». Non, non, non. D'abord, il n'existe pas un seul serveur racine mais plusieurs (leur nombre dépend de comment on compte `<https://www.bortzmeyer.org/combien-serveurs-racines.html>`) et, surtout, la clé en question est tout simplement la clé de signature des données situées à la racine des noms de domaine. Elle ne contrôle pas une machine mais des données.

Revenons maintenant à la propriété la plus importante de DNSSEC, le fait qu'il soit optionnel. Ce point est complètement oublié dans l'article, parce que cela obligerait à dire que cette fameuse clé n'est pas si importante que cela, puisque seuls les gens qui utilisent DNSSEC pourraient éventuellement être affectés par sa perte ou son vol. Et l'infographie dans l'article cite un seul exemple de « nom de domaine sécurisé »... `gqmagazine.fr` qui justement ne l'est **pas**. Ce nom n'est pas signé avec DNSSEC et la perte ou le vol des clés de la racine n'auraient donc rigoureusement **aucune** influence sur la sécurité de GQ.

La partie de l'article concernant la gouvernance n'est pas épargnée, avec une affirmation comme quoi l'ICANN « définit également les protocoles qui permettent aux machines de communiquer entre elles » (c'est faux, c'est le rôle de l'IETF).