

[Histoire] Le protocole finger et la vie privée

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 août 2022

<https://www.bortzmeyer.org/finger-vie-privee.html>

Sur le fédivers, jonny <<https://social.coop/@jonny>> a attiré l'attention sur une discussion un peu oubliée, qualifiée avec une certaine exagération de « une des premières polémiques sur Internet ». Il s'agissait d'un débat en 1979 sur un changement technique fait dans des serveurs finger pour protéger un peu la vie privée, changement qui n'avait pas fait consensus. Un sujet toujours d'actualité, même dans l'Internet très différent que nous avons aujourd'hui.

Pour comprendre le débat, il faut passer un paragraphe à expliquer finger. Normalisé (mais bien après les faits) dans le RFC 1288¹, finger était un service d'information très populaire, qui permettait de trouver des informations sur un utilisateur d'une machine distante, son numéro de téléphone, son adresse postale, s'il était connecté en ce moment, etc. Avec les yeux d'aujourd'hui, on voit bien les questions de vie privée que cela peut poser. Le changement qui avait été fait dans un serveur finger (à l'université Carnegie-Mellon) était de ne pas diffuser l'information la plus sensible (dernière connexion, et dernière lecture du courrier électronique) par défaut (mais l'utilisateur avait une option pour activer cette diffusion).

Et c'est là que la polémique, en 1979, a commencé. Vous pouvez lire l'archive de la liste de diffusion msggroup de l'époque <<http://mercury.lcs.mit.edu/~jnc/tech/msggroup/msggroup0701-0800.txt>> et voir la discussion de nos jours suite au pouète de jonny <<https://social.coop/@jonny/108750221723317464>>. Quel était le problème avec le changement fait à Carnegie Mellon? C'était que ne pas diffuser l'information semblait à beaucoup anti-social. Le débat semble assez surréaliste aujourd'hui, avec une forte pression sociale pour tout diffuser par défaut. Mais, comme le notent Arne Babenhauserheide et Antoine-Frédéric dans la discussion, les mécanismes permettant d'indiquer qu'un message a été lu (qui sont déployés par exemple par WhatsApp) posent presque les mêmes problèmes (l'information n'est pas publique toutefois).

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc1288.txt>

La loi Informatique & Libertés existait déjà, pourtant, mais on peut penser qu'elle n'était pas connue du petit groupe qui faisait alors fonctionner l'Internet, et au sein duquel tout le monde était à la fois utilisateur et acteur.

Il y a plein de choses à remarquer dans cette discussion. D'abord, que des choix apparemment très techniques (deux bits dans la configuration pour indiquer si on diffuse ces deux informations) sont en fait politiques. La passion déclenchée par ce simple changement (qui concernait un seul serveur finger : ceux qui n'étaient pas d'accord n'étaient pas obligés de modifier le leur) montre bien que tout le monde était conscient de l'importance de la question. Notons toutefois que des opposants au changement fait par l'université affirmaient que c'était un changement « politique », manifestement en considérant que ce terme était une insulte.

Ensuite, on peut noter bien sûr que les mentalités ont changé : on n'imagine plus aujourd'hui affirmer que garder ces informations privées est anti-social. Mais les changements ne sont pas si importants que cela ; encore aujourd'hui, lorsqu'on dénonce des atteintes à la vie privée, il y a toujours quelqu'un pour dire « si vous ne faites rien de mal, vous n'avez pas de raison d'avoir une vie privée ».

À propos de mentalité, il y a un cliché courant aujourd'hui qui est de dire que l'Internet n'avait pas été conçu pour la sécurité, c'est parce que, à l'époque, ses utilisateurs/acteurs étaient tous des hippies barbus et universitaires qui vivaient dans un monde de bisounours et se faisaient confiance. Il est vrai que ce monde était assez restreint, avec une forte homogénéité de classe sociale, de pays (uniquement des étatsuniens), de profession et de mentalité. Et l'espoir était en effet qu'une mentalité d'ouverture, de franche discussion et de confiance allait se généraliser. Ce n'était bien sûr pas réaliste, un tel climat pouvait se maintenir dans un petit groupe cohérent, mais avait peu de chance de passer à l'échelle, dans un Internet aux dimensions du monde. (Ceci dit, je préfère l'optimisme, même erroné, au cynisme « de toute façon, c'est la nature humaine, la loi de la jungle, la société sera toujours violente, et il faut mettre des barbelés partout ».)

Mais si les acteurs de l'Internet de l'époque sous-estimaient les questions de sécurité, ils ne les ignoraient pas. Sur bien des points où on reproche aux pionniers de l'Internet de n'avoir pas pris en compte la sécurité dès le début, il faut remarquer que, d'abord, il y a des bonnes raisons pour ne **pas** encombrer un nouveau système avec de la sécurité, si on veut qu'il soit un succès (RFC 5218). Ensuite, même aujourd'hui, avec l'expérience et le recul, on serait bien en peine de déployer un système sécurisé à l'échelle mondiale, avec le cahier des charges de l'Internet, qui est notamment de permettre à toute Alice de parler à tout Bob. Bref, les questions de 1979 n'appartiennent pas à un passé définitivement révolu, elles se posent toujours aujourd'hui.

Et un autre point à noter : l'importance de la valeur par défaut. Le changement fait à Carnegie Mellon impactait tous les utilisateurs (je n'utilise pas l'écriture inclusive ici car je soupçonne qu'il y avait peu d'utilisatrices), à part la minorité qui change les réglages. Ce problème est toujours d'actualité, par exemple lorsque Facebook se défend des reproches sur son manque de protection de la vie privée en disant que les utilisateurices peuvent toujours changer les réglages (tout en sachant que très peu le feront).