# L'IETF et l'espionnage, et maintenant ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 novembre 2013

https://www.bortzmeyer.org/ietf-securite-espionnage-bis.html

---

J'ai déjà parlé ici <https://www.bortzmeyer.org/ietf-securite-espionnage.html> de l'attitude de l'IETF face à l'espionnage massif ("*pervasive surveillance*" est le terme le plus répandu à l'IETF) auquel se livrent des organisations comme la NSA. Maintenant que la réunion IETF de Vancouver est bien avancée, quelles vont être les suites ?

Quelques informations sur la plénière technique du 6 novembre, qui a symboliquement marqué le passage de l'IETF en mode « on est vraiment fâchés ». Les documents, diapos, etc sont tous en ligne <https://datatracker.ietf.org/meeting/88/materials.html#wg-plenaryw>. La plénière a été filmée et le film est aussi en ligne <https://www.youtube.com/watch?v=oV71hhEpQ20> (chez un fournisseur de PRISM, ce qui est amusant). La partie sur la surveillance commence après 23 minutes environ quand Alissa Cooper, auteure du RFC 6973 [1], monte à la tribune.

La vedette était Bruce Schneier, qui a bien fixé les objectifs : empêcher toute surveillance n'est pas réaliste, ce contre quoi on peut lutter, c'est la surveillance de masse. Schneier a posé le problème en termes financiers : la surveillance est trop bon marché aujourd'hui et peut donc être faite massivement. Des réformes techniques pourraient contribuer à la rendre plus coûteuse, forçant les agences d'espionnage à revenir à de la surveillance ciblée, ce qui serait mieux que rien. Il a également insisté sur le « partenariat public/privé » : la NSA ne fait pas tout toute seule, elle est aidée par les géants du Web, qui lui fournissent des données (c'est un des points dont l'IETF, où des entreprises comme Google sont très présentes, n'aime pas discuter, et cela explique certains manques dans le RFC 6973).

Du point de vue pratique, Schneier a rappelé l'importance de l'ergonomie (ne pas fournir d'options dans les logiciels de sécurité, car elles seront mal utilisées), et de la sécurité par le nombre (si peu de gens utilisent le chiffrement, celui-ci est négatif, il attire l'attention sur eux ; il faut du chiffrement massif).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6973.txt

Brian Carpenter a fait l'historique des RFC parlant de vie privée, du RFC 1126 (le premier à parler de sécurité... pour dire qu'il ne s'en occuperait pas) puis au RFC 1543, qui a rendu obligatoire la fameuse section "*Security Considerations*". Il a aussi rappelé le contexte notamment la lutte de certains pays (la France a été citée) contre la cryptographie dans les années 80 et 90.

Stephen Farrell est ensuite passé au concret : que peut faire l'IETF ? (Il a aussi illustré son exposé d'une jolie photo d'un parc mais il aurait pu choisir de l'herbe.) Le nouveau groupe IETF perpass <https://www.ietf.org/mailman/listinfo/perpass> (abréviation de "*pervasive passive monitoring*") est chargé de trier les idées : le travail concret se fera ensuite dans des groupes de travail spécialisés. L'orateur a noté la menace particulière que faisait planer l'Internet des objets : « la NSA saura quand vous tirez la chasse ».

Enfin, les chercheurs en sécurité noteront l'annonce d'un atelier de l'IAB « "*Internet Hardening*" » à Londres le 28 février 2014. Préparez vos articles !

La plénière technique à l'IETF n'est pas composée que d'exposés formels mais contient aussi une discussion. Cooper a introduit cette discussion en appelant les membres de l'IETF à la responsabilité (« plein de gens vous écoutent », ce qui a fait éclater la salle de rire). De nombreux thèmes ont été abordés : vue la disproportion des moyens, pouvons-nous vraiment gêner la NSA (Schneier : « oui, ils ont des limites, ne serait-ce que les lois de la physique »), intérêt de disperser les services à surveiller (il est plus coûteux de surveiller 100 000 serveurs de messagerie qu'un seul Gmail), et même l'argument très traditionnel « mais on n'est pas des terroristes, on n'a rien à cacher » (Cooper : « on veut de la vie privée même pour des activités légales, songez à vos visites chez le docteur, par exemple »)

La proposition de « durcir l'Internet <http://www.ietf.org/blog/2013/11/strengthening-the-inter > » pour rendre la surveillance moins facile a été largement adoptée, par la pittoresque procédure du « hum ». Sans surprise, le communiqué officiel <http://www.ietf.org/media/2013-11-07-internet-priv html> prend acte de ce consensus et s'en félicite. Mais cela ne veut pas dire que tout se passera comme sur des roulettes après. Il y a eu des critiques (plus ou moins voilées) contre ce projet (personne n'ose s'y opposer frontalement mais cela n'empêche pas les attaques indirectes) et, surtout, voter des motions est facile, développer de nouvelles techniques et protocoles et les déployer est une autre histoire.

Ce sera justement le premier travail du groupe perpass <https://www.ietf.org/mailman/listinfo/perpass>. Il s'est réuni juste après la plénière et avait un agenda chargé ! (Les documents sont eux aussi en ligne <https://datatracker.ietf.org/meeting/88/materials.html#perpass>). Dave Thaler a notamment fait un remarquable exposé sur l'état des menaces sur la vie privée. Cet exposé tordait le cou à la légende très répandue comme quoi les cybercriminels auraient la partie trop facile, l'Internet leur permettrait l'anonymat, etc. C'est tout le contraire : la vie privée est aujourd'hui extrêmement difficile à préserver dans les réseaux numériques.

Et les solutions envisagées ? L'IETF a plein d'idées :

— Évidemment, généraliser le chiffrement. Les gens de XMPP se sont promis de le faire pour leur protocole de messagerie instantanée avant mai 2014 <https://github.com/stpeter/manifesto>.
— Un terme souvent revenu dans les discussions est celui d'"*opportunistic encryption*". Il n'est pas très rigoureusement défini. Des fois, il veut dire « chiffrement sans authentification préalable » (ce qui protège d'un attaquant passif mais pas d'un homme du milieu), des fois, il signifie « chiffrement sans configuration manuelle préalable » et, là, c'est très souhaitable si on veut avoir des chances de généraliser le chiffrement.
— Minimisation des données envoyées. Le chiffrement ne protège pas si le destinataire transmet vos données à un tiers (cas de Facebook, par exemple). Il est donc également nécessaire de diminuer la quantité de données envoyées. Christian Huitema a ainsi lancé un appel à ce que les résolveurs DNS arrêtent d'envoyer la question complète aux serveurs faisant autorité.

---

https://www.bortzmeyer.org/ietf-securite-espionnage-bis.html

Alissa Cooper a bien résumé la démarche perpass : « 1) envoyer le moins de données possibles 2) les chiffrer ». Il n'y a plus qu'à réaliser ce programme.

Y a-t-il consensus sur cette démarche ? Comme indiqué plus haut, les opposants se font très discrets. Mais certaines remarques négatives ont déjà été entendues, par exemple que la généralisation du chiffrement de bout en bout va empêcher les intermédiaires d'examiner ou de modifier les messages (ce qui me semble une bonne chose mais ce n'est pas l'opinion de tout le monde, d'autant plus qu'il y a des craintes que les attaquants s'adaptent et cherchent d'autres moyens) ou, autre exemple, que la gestion opérationnelle des réseaux va en souffrir (un ennui courant avec la cryptographie <https://www.bortzmeyer.org/crypto-debug.html>).

Et puis, même si tout le monde est d'accord, le principe de réalité ne manquera pas de frapper : certains des changements proposés auront un coût et certains, qui ont applaudi avec enthousiasme à la proposition de renforcer la sécurité de l'Internet, reculeront peut-être devant ce coût.

D'autres articles intéressants sur cette question :

— Deux très bons articles de Tim Bray sur l'état de la sécurité Internet <https://www.tbray.org/ongoing/When/201x/2013/11/04/State-of-internet-security> (et notamment le tour d'horizon des applications existantes, question chiffrement) et sur le cas spécifique de HTTP <https://www.tbray.org/ongoing/When/201x/2013/11/05/IETF-88-HTTP-Security>.
— Les notes de Gwen Wiley <http://gwiley.com/ietf88_gwiley_notes_20131106.txt>, plutôt brutes de fonderie.
— Un bon compte-rendu de Technology Review <http://www.technologyreview.com/view/521306/time-for-internet-engineers-to-fight-back-against-the-surveillance-internet/>.
— L'article du Economist <http://www.economist.com/news/science-and-technology/21589383-stung-revelations-ubiquitous-surveillance-and-compromised-software>.
— Un bon résumé <http://blog.does-not-exist.org/2013/11/10/ietf88-on-the-costs-of-pervasi> notant à juste titre qu'il n'y avait jamais eu de réunion IETF aussi focalisée sur un seul point.
— Le RFC 7258, publié quelques mois après la réunion de Vancouver, et qui résume la politique de l'IETF sur cette question.