RFC 7258 : Pervasive Monitoring Is an Attack

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 mai 2014

Date de publication du RFC : Mai 2014

http://www.bortzmeyer.org/7258.html

Assez des RFC qui décrivent un protocole réseau, jusque dans les plus infimes détails, au bit près ? Et des RFC bureaucratiques sur le fonctionnement de l'IETF et de tout son zoo de groupes et de comités ? Voici un RFC 100 % politique, et un excellent, en plus. Ce RFC 7258 [1] résume la politique de l'IETF vis-à-vis de l'espionnage de masse que pratique, entre autres, la NSA : cet espionnage de masse est, techniquement, une attaque, et il est justifié de faire tout ce qu'on peut techniquement pour combattre cette attaque.

Cette affirmation n'allait pas de soi. Rappelez-vous qu'un des mécanismes utilisés par la NSA (et révélé par le héros Snowden) pour faciliter l'espionnage est justement d'affaiblir les systèmes de sécurité, au nom du « il faut bien que nous, qui sommes les gentils, puissions écouter les plans des méchants pédonazis ». (C'est notamment le programme BULLRUN.) Après quelques discussions, l'IETF affirme haut et fort que cet argument ne tient pas : si on affaiblit la sécurité du réseau pour faciliter les écoutes légales, on l'affaiblit face à tous les espions, qu'on les trouve légitimes ou pas.

Avant de faire face à une attaque, il faut la définir. Notre RFC considère (section 1) que l'espionnage de masse (PM pour "*Pervasive Monitoring*") est une attaque d'un nouveau genre. Ce n'est plus simplement le lycéen dans son garage qui écoute un réseau Wi-Fi proche et mal protégé. L'espionnage de masse n'est pas une nouveauté technique (les révélations de Snowden ne contiennent aucune surprise technique, aucune technique ultra-avancée, genre X-Files) mais se distingue des attaques précédentes par son caractère indiscriminé (on écoute tout le monde, innocent ou coupable, avant même tout soupçon), et sa simple taille (la STASI, avec les moyens techniques de l'époque, devait choisir qui elle écoutait ; la NSA peut, grâce aux méthodes de traitement du "*big data*", écouter tout le monde).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7258.txt

L'espionnage de masse est défini comme l'écoute à très grande échelle des communications sur le réseau (qu'on se limite aux métadonnées ou pas), en utilisant des mécanismes passifs (l'écoutant traditionnel des analyses de risque), ou actifs (le programme Tailored Access Operations avec son QUANTUM et son FOXACID).

L'IETF a considéré depuis le début que l'espionnage massif était une attaque contre la vie privée. La question a fait l'objet de beaucoup de débats <http://www.bortzmeyer.org/ietf-securite-espionnage.html> à la réunion IETF de Vancouver en novembre 2013, débats qui ont donné lieu à plein de bonnes résolutions <http://www.bortzmeyer.org/ietf-securite-espionnage-bis.html> (cf. les documents de la session plénière <http://www.ietf.org/proceedings/88/>). Pour les résumer : l'IETF doit modifier ses protocoles réseau et concevoir les futurs protocoles de manière à rendre l'espionnage plus difficile. Le rendre impossible est sans doute irréaliste (et, certains le pensent, non souhaitable, car ils estiment que la surveillance ciblée, par exemple d'un suspect par la police, doit rester possible). L'idée est donc plutôt de rendre la surveillance de masse si difficile, et donc si coûteuse, que les organisations qui écoutent devront se limiter à une écoute ciblée sur les seules personnes sur lesquels pèsent des soupçons sérieux. « "*Don't give them anything for free.*" »

Le mot « attaque » est utilisé par l'IETF dans un sens purement technique (cf. RFC 4949 pour de la terminologie) : il s'agit d'une action délibérée par un tiers pour remettre en cause les attentes des deux parties qui communiquent (ici, leur attente que la communication soit privée), et il n'implique rien quant à la légitimité ou la légalité de telles attaques. Une attaque peut donc être légale, elle pose néanmoins exactement les mêmes problèmes techniques, et nécessite les mêmes solutions. Il serait ridicule de croire qu'on pourrait concevoir des systèmes de sécurité qui empêchent les « méchants » d'écouter mais autoriseraient les « gentils ». Quelle que soit l'opinion qu'on a sur ces « gentils », il est important de garder en tête qu'on ne peut pas se protéger contre les « méchants » sans bloquer ou gêner aussi les écoutes des « gentils ». Toute l'approche de l'IETF est techniquement neutre, dans le sens où on ne se préoccupe pas des motivations des espions : ceux-ci peuvent être une puissante agence gouvernementale, une entreprise commerciale qui veut récolter de l'information sur ses clients (ce qui peut être légal dans certains pays), un gang de délinquants dans leur sous-sol, ils peuvent agir pour le fric, l'idéologie, le goût du pouvoir ou n'importe quelle autre raison : c'est le même problème technique et les solutions seront les mêmes.

Après ces préalables, la section 2 du RFC décrit la position de l'IETF : on va travailler pour limiter l'espionnage de masse. On l'a vu, le rendre complètement impossible est sans doute peu réaliste. L'idée, suivant l'exposé de Schneier à la réunion de Vancouver, est d'augmenter les coûts pour l'attaquant, le forçant à mieux cibler ses opérations, et/ou exposant de l'espionnage qui serait resté caché autrement.

Les protocoles IETF avaient déjà souvent des mécanismes permettant de protéger la vie privée, typiquement du chiffrement afin d'empêcher un tiers d'accéder aux données échangées. Ces mécanismes sont recommandés par le RFC 3552. Mais ils ne prennent pas en compte le changement de catégorie que représente l'espionnage de masse. Le chiffrement, en général, ne protège pas les métadonnées, il ne tient pas compte des risques d'analyse de trafic, et il ne protège pas si les extrémités de la communication trahissent (cas du programme PRISM), ce qui nécessiterait une minimisation des données, pas uniquement leur chiffrement. Il est donc nécessaire d'adapter les normes de la famille TCP/IP, suivant la prise de conscience qui a suivi les révélations d'Edward Snowden.

En pratique, notre RFC demande aux auteurs de protocoles de prendre en considération le risque d'espionnage massif. Cela n'implique pas forcément une section « "*Pervasive Monitoring Considerations*" » dans leur RFC (comme il existe une « "*Security Considerations*" » obligatoire). Mais cela veut dire que les auteurs doivent regarder la question et être prêt à répondre aux questions à ce sujet. (Ce point était l'un des plus contestés lors de la création de ce RFC : certaines versions étaient plus directives, imposant des contraintes moins vagues.) En matière de lutte contre l'espionnage massif, comme

souvent en sécurité, il vaut mieux prévoir les protections dès qu'on conçoit l'architecture, les mettre après est souvent très complexe.

À propos de complexité, une des difficultés de la lutte contre l'espionnage massif est qu'on a toujours besoin de gérer ses réseaux et que certaines activités de gestion sont proches de l'espionnage (surveiller les caractéristiques du trafic à partir de NetFlow, par exemple, ou bien utiliser tcpdump pour déboguer une application <http://www.bortzmeyer.org/crypto-debug.html>). Il serait dommage que les mesures techniques de protection de la vie privée bloquent ces pratiques. En fait, il y a même des mesures de sécurité qui reposent sur la publication, comme la "*Certificate Transparency*" du RFC 6962 (ou comme, mais le RFC ne le cite pas, Bitcoin). Il y a donc là un difficile compromis à négocier.

Enfin, la section 2 du RFC rappelle que l'IETF a des pouvoirs limités : c'est une SDO, elle écrit des normes, elle ne fait pas les programmes qui mettent en œuvre ces normes, encore moins les pratiques de déploiement et de sécurité. (Sans même mentionner les activités politiques et juridiques, qui sont encore plus loin de l'IETF.) Or, la sécurité (vie privée ou autre) dépend bien plus des programmes et des pratiques que des normes techniques.

La section 3 du RFC résume ce qui a déjà été fait à l'IETF, et le processus suivi : les RFC 1984 et RFC 2804 étaient déjà des déclarations technico-politiques sur la sécurité, et avaient été faits en commun entre l'IAB et l'IESG. L'IETF ayant changé ses règles bureaucratiques internes depuis, ce RFC 7258 est publié par l'IETF, sans l'IAB. C'était également le cas du RFC le plus complet sur la vie privée, l'excellent RFC 6973, dont la lecture est très recommandée.