RFC 7624 : Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 septembre 2015

Date de publication du RFC : Août 2015

https://www.bortzmeyer.org/7624.html

La publication, grâce à Edward Snowden, d'affreux PowerPoint[Caractère Unicode non montré [1]] de la NSA montrant l'ampleur de la surveillance permanente et généralisée a suscité une prise de conscience chez tous les acteurs de l'Internet. (D'autant plus que d'autres pays en font autant, comme la France, surtout depuis la Loi Renseignement.) Ces PowerPoint[Caractère Unicode non montré] sont souvent d'interprétation difficile et il est donc nécessaire, lorsqu'on travaille aux contre-mesures, d'avoir un modèle clair de la menace contre laquelle on tente de défendre les citoyens internautes. Ce nouveau RFC est l'une des étapes dans ce travail à l'IETF : décrire clairement les risques de la surveillance généralisée.

Ce RFC est écrit par l'IAB, et on note parmi les auteurs Bruce Schneier. Il ne s'agit pas de revenir sur le problème bien connu de l'espionnage des communications (qui est aussi ancien que les réseaux), mais sur les nouveautés qui résultent de la prise de conscience d'un espionnage illimité et indiscriminé (cf. RFC 7258 [2] pour la décision politique de considérer cet espionnage comme une attaque contre l'Internet). Les programmes de la NSA, avec leurs noms rigolos, n'utilisent pas de vulnérabilités inconnues. Aucune science-fiction derrière PRISM, TEMPORA ou BULLRUN. Ces programmes exploitent uniquement des risques connus, mais de manière massive, avec un budget très élevé et une absence totale de scrupules.

Notre nouveau RFC commence donc logiquement par un peu de terminologie (section 2). Il réutilise d'autre part les précédents RFC analogues notamment celui de terminologie de la sécurité (RFC 4949) et celui d'analyse de la protection de la vie privée (RFC 6973). Notons deux choses importantes : d'abord la distinction entre attaques **passives** et **actives**. La différence ne vient pas de l'effort de l'attaquant (monter une attaque passive peut être beaucoup de travail) mais du fait que, dans le premier cas, l'attaquant

1. Car trop difficile à faire afficher par LaTeX
2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7258.txt

n'écrit rien sur le réseau, n'envoie aucun paquet, ne stoppe aucune communication et ne modifie aucun bit. Il espionne, c'est tout. Au contraire, dans une attaque active comme QUANTUM, le surveillant se permet d'interférer avec les communications, changeant le contenu d'un paquet, envoyant des paquets (pour de l'"*ARP spoofing*" par exemple, ou de l'empoisonnement de cache DNS), bloquant certains paquets (par exemple pour faire une attaque par repli contre TLS).

Et la deuxième chose importante est le terme relativement nouveau d'**attaque généralisée** ("*pervasive attack*"), qui désigne les attaques menées, non pas par le lycéen dans son garage, mais par un organisme puissant, pouvant observer (et peut-être intervenir) en de très nombreux points du réseau, avec des capacités "*big data*".

Commençons par décrire l'attaquant, étape indispensable pour élaborer un modèle de menace (section 3). D'abord, un modèle d'un attaquant purement passif (et donc moins puissant que la NSA). S'il est purement passif, cet attaquant « idéal » (idéal du point de vue du modèle, pas du point de vue légal ou moral) a quand même de grandes possibilités, notamment quantitatives. Il voit tout, partout. Le RFC note à juste titre qu'avant les révélations de Snowden (qu'on ne remerciera jamais assez pour ce qu'il a fait), un tel attaquant aurait été considéré comme le produit d'un esprit à la limite de la paranoïa, à part chez les experts en sécurité (qui se doutaient bien, même avant Snowden, de la réalité de la surveillance massive). Cet attaquant peut notamment :

— Observer tous les paquets, où qu'ils passent,
— Observer les données stockées dans les différentes machines (comme le permet PRISM),
— Collaborer avec d'autres attaquants (comme le font les "*Five Eyes*"),
— Mais ne peut pas bloquer, modifier, injecter, il est purement passif.

L'attaquant doit donc se débrouiller avec ce qu'il observe directement, puisqu'il ne peut pas le modifier, et ce qu'il en déduit (**inférence**, c'est-à-dire dériver des informations de celles qu'on a déjà).

Le chiffrement, même sans authentification, protège largement contre un tel attaquant, en réduisant sérieusement les observations qu'il peut faire. (À condition que ce chiffrement soit bien réalisé, par exemple que les générateurs aléatoires soient de qualité. Cette condition est, en pratique, très difficile à remplir.) Le chiffrement est par contre moins efficace contre l'inférence. Par exemple, les fameuses métadonnées laissées en clair (en-têtes IP et TCP lorsqu'on utilise TLS) peuvent donner plein d'information. Un autre exemple est la taille des paquets (qui permet de savoir si on a envoyé ou reçu un fichier), une information que TLS (ou SSH) ne brouille pas. Même IPsec/ESP, s'il chiffre l'en-tête de couche 4, laisse la couche 3 (IP) en clair.

L'idéal bien sûr pour notre attaquant modèle est quand il n'y a pas de chiffrement. Quand tout est en clair, le contenu des communications est accessible trivialement. Voilà pourquoi le RFC 3365 (en 2002 ! Ça ne nous rajeunit pas.) disait déjà que tout protocole IETF susceptible d'envoyer des données en clair doit avoir une version sécurisée qui chiffre. C'est le cas de presque tous les protocoles aujourd'hui. Le RFC note qu'il y a une exception avec le DNS mais elle est en train d'être comblée par le groupe de travail DPRIVE <https://tools.ietf.org/wg/dprive>, (cf. le RFC 7626).

L'inférence peut aussi utiliser des informations qui se trouvent dans des bases de données extérieures à la communication elle-même. Par exemple, comme l'ICANN impose de publier les coordonnées des titulaires des noms de domaine dans les TLD qu'elle contrôle, ces informations peuvent nourrir l'inférence. Même chose avec les bases géoIP ou, encore mieux, avec la quantité d'informations disponibles dans des réseaux sociaux comme Facebook. Ces dernières sources sont très riches, avec de l'information déjà structurée et envoyée « volontairement » par les utilisateurs. Cela met une sérieuse limite à ce que l'IETF peut faire pour améliorer la vie privée sur l'Internet : améliorer les protocoles n'est pas suffisant.

Notre RFC détaille comment inférer à partir des observations directes. Par exemple, pour corréler des adresses IP avec des utilisateurs, on a plusieurs outils : une requête DNS « inverse » (type PTR) suffit

parfois. Ces requêtes marchent bien pour les serveurs, peu nombreux et stables (donc une copie locale peut être facilement faite, pour accélerer le processus). Elles sont moins efficaces pour les clients (on obtient parfois des trucs sans trop d'intérêt comme `ARouen-655-1-102-140.w90-23.abo.wanadoo.fr`). Notez que le RFC étudie les possibilités de surveillance **massive**. La technique (légale dans de nombreux pays démocratiques) qui consiste pour la police à demander au FAI le nom de l'utilisateur correspond à telle adresse IP ne marche pas ici, elle ne passe pas à l'échelle. C'est un exemple de la différence entre enquêtes ciblées et surveillance généralisée, style Big Brother.

Même si le FAI ne coopère pas dans la mission de surveillance, il existe d'autres moyens de relier une adresse IP à des identités de l'utilisateur. Par exemple, s'il utilise IMAP, on a facilement son identificateur, sauf si la session est chiffrée (ce qui n'est pas encore fait partout). Le problème n'est pas spécifique à IMAP et se trouve aussi dans SIP et dans bien d'autres protocoles. Chiffrer la session n'est donc pas uniquement utile lorsqu'on a « quelque chose à cacher » mais aussi simplement lorsqu'on veut éviter d'être suivi à la trace. Un autre exemple amusant est décrit en section 3.3.4 : l'utilisation des entêtes `Received:` du courrier. Même si tout le courrier est chiffré, l'attaquant peut toujours s'abonner à des listes de discussion publiques comme perpass <`https://www.ietf.org/mailman/listinfo/perpass`>. Il reçoit alors des messages avec ce genre d'en-têtes :

```
Received: from 192-000-002-044.zone13.example.org (HELO ?192.168.1.100?) (xxx.xxx.xxx.xxx) by lvps192-000-002-21
   with ESMTPSA (DHE-RSA-AES256-SHA encrypted, authenticated); 27 Oct 2013 21:47:14 +0100
Message-ID: <526D7BD2.7070908@example.org>
Date: Sun, 27 Oct 2013 20:47:14 +0000
From: Some One <some.one@example.org>
```

Collectionner ces en-têtes va lui permettre de compiler une base des émetteurs et des adresses IP qu'ils utilisent. Au bout d'un moment, l'attaquant saura que, si un paquet IP vient de `192.0.2.44`, il y a de fortes chances que ce soit l'utilisateur Some One.

Parmi les techniques d'inférence, il y a aussi celles fondées sur les graphes de relations. Si une adresse IP envoie X % de ses paquets à l'IETF, Y % au MIT et Z % à YouPorn, l'observation ultérieure d'une toute autre adresse IP qui a le même graphe de relations peut permettre de conclure que la même personne est derrière les deux adresses.

Il y a aussi les adresses MAC. Celles-ci sont uniques au niveau mondial et sont en général très stables (peu de gens utilisent macchanger <`https://github.com/alobbs/macchanger`>). Si le réseau est publiquement accessible (ce qui est typiquement le cas des "*hotspots WiFi*"), l'attaquant peut facilement regarder « qui est là » et mettre à jour sa base de données. Notez que certaines techniques, comme les SSID cachés aggravent le risque : la machine de l'utilisateur va diffuser les SSID qu'elle cherche, donnant ainsi davantage d'informations à l'attaquant. Des bases de données des "*hotspots*" existent déjà (constituées, par exemple, par les utilisateurs d'Android, dont le smartphone transmet à Google et à la NSA plein d'informations sur les SSID détectés). C'est évidemment encore plus facile pour l'attaquant si le réseau WiFi n'utilise pas WPA ou équivalent (tapez sur votre fournisseur WiFi si ce n'est pas le cas).

Ce très intéressant exposé des techniques d'espionnage existantes est évidemment incomplet : nul doute que la NSA ou la DGSI ont plein d'autres idées. Et il y a certainement des différences entre la théorie de la section 3 et la réalité de la surveillance massive effectuée par ces organisations. Il est bien sûr impossible de savoir exactement ce que la NSA sait faire <`https://www.bortzmeyer.org/security-day-nsa.html`>. Tout au plus peut-on faire quelques suppositions raisonnables (section 4 de notre RFC). D'abord, les révélations Snowden ne laissent pas de doute sur l'existence de cette surveillance généralisée effectuée par la NSA et le GCHQ (notez que notre RFC ne fait pas dans la fausse

pudeur, et cite les noms de ces organisations, alors qu'avant on ne parlait que de « certaines agences gouvernementales »). Ensuite, ces mêmes révélations donnent une première idée des méthodes utilisées. Et il n'y a pas que la NSA et ses collaborateurs : nul doute que les services secrets français, chinois, russes ou israéliens espionnent également massivement, dans la mesure de leurs moyens matériels et de leurs compétences. Mais on n'a pas encore les détails, on attend un héros comme Snowden dans ces pays moins imbibés de culture démocratique.

Donc, "*reality check*", à la lumière des révélations Snowden, que fait effectivement la NSA, par rapport à l'attaquant passif idéalisé de la section 3 ? D'abord, cette organisation d'espionnage a effectivement une activité massive de collecte passive :

— Son système XKEYSCORE surveille l'Internet depuis un très grand nombre de points de mesure, à la recherche d'élements indiquant une cible (comme une adresse de courrier particulière),
— Le programme TEMPORA du GCHQ espionne les câbles sous-marins (environ 1 500 d'entre eux),
— Et on peut aussi citer MUSCULAR, qui se branche sur les câbles reliant les différents centres de données de gros acteurs Internet, pour capturer leur trafic interne.

Ce n'est pas tout de capturer, il faut aussi décoder, et une partie du trafic est chiffré. La NSA ne renonce pas devant le chiffrement et, par exemple, son programme BULLRUN met en œuvre divers moyens pour affaiblir la protection qu'offre la cryptographie, par exemple par des modifications du code.

Et, surtout, la NSA ne se contente pas d'attaques passives, comme le faisait l'attaquant modélisé en section 3. Elle a aussi des mécanismes actifs :

— Attaques de l'homme du milieu par exemple par des modifications des réponses DNS ou HTTP non sécurisées (programme QUANTUM),
— Piratage des ordinateurs des utilisateurs (système FOXACID, outils comme ceux que vend Hacking Team aux dictateurs),
— Piratage des routeurs, comme décrit dans cet article du Spiegel <http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-nee
html>,
— Utilisation de botnets (autre article du Spiegel <http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-101
html>),
— Et détournement des normes techniques de façon à les affaiblir sérieusement, comme la NSA l'a fait avec le générateur aléatoire de Dual EC DRBG. (Là aussi, l'IAB ne prend pas de gants et cite des noms comme RSA security, accusée d'avoir utilisé ce générateur en le sachant compromis.) Ce point est évidemment particulièrement crucial pour l'IETF, elle-même organisme de normalisation et qui doit donc désormais bien faire attention à toutes les « contributions », certaines d'entre elles pouvant être des attaques contre le nouveau protocole.

Si les révélations Snowden ne portent que sur la NSA et le GCHQ, le RFC rappelle que d'autres États n'hésitent certainement pas à recourir aux mêmes méthodes, et le cas évident de la Chine est cité, avec les techniques de modification de données utilisées par le GFW, techniques qui rappellent fortement le QUANTUM états-unien. Par exemple, le réseau chinois n'hésite pas à modifier les réponses DNS <https://www.bortzmeyer.org/detournement-racine-pekin.html>. De l'espionnage actif à l'attaque par déni de service, il n'y a qu'un pas, que le gouvernement chinois a franchi avec le Grand Canon <https://citizenlab.org/2015/04/chinas-great-cannon/> et peut-être avec l'attaque « Poivre du Sichuan » <https://www.bortzmeyer.org/sichuan-pepper.html>.

La section 5 de notre RFC synthétise la menace à laquelle nous devons désormais faire face. Les attaquants comme la NSA ou la DGSE peuvent :

— Effectuer passivement des observations (cf. la section 3),
— Inférer, à partir des observations,
— Contrairement à l'attaquant passif de la section 3, ces organisations peuvent aussi faire des attaques actives,

— La cryptographie ne protège pas dans 100 % des cas : entre autres contre-mesures, ces organisations peuvent obtenir des clés privées, soit ponctuellement (piratage d'un ordinateur, fausse manœuvre de l'utilisateur), soit systématiquement (faille de sécurité délibérement introduite dans le logiciel via BULLRUN, piratage d'un fournisseur <https://theintercept.com/2015/02/19/great-sim-heist>),
— Et, enfin, obtenir les données stockées, ce que le chiffrement de la communication n'empêche pas (programme PRISM, où des collaborateurs de la NSA comme Google lui donnent accès à leurs données).

La traditionnelle opposition attaquant passif / attaquant actif des analyses de sécurité est sans doute insuffisante dans le cas de la surveillance systématique. Les trois dernières possibilités citées plus haut (obtention ponctuelle des clés, obtention systématique des clés et accès aux données stockées) étaient ainsi absentes ou très sous-estimées, avant Snowden. En outre, comme ces trois possibilités se situent en dehors des protocoles réseau, l'IETF tendait à les négliger, les considérant comme hors de son domaine.

Autrefois, on considérait que les attaquants actifs étaient forcément situés en bordure du réseau : sur un "*hotspot*" WiFi non protégé par WPA, une attaque active est triviale, pour toute personne connectée à ce "*hotspot*". Mais les organisations comme la NSA peuvent également agir au cœur de l'Internet, ce qui augmente sérieusement leurs possibilités. J'avais entendu lors d'une conférence de sécurité un expert affirmer qu'il ne fallait jamais utiliser la WiFi mais toujours la 3G pour des raisons de sécurité. Ce conseil peut avoir un sens face à un attaquant lycéen dans son garage mais certainement pas face à des organisations importantes, pour qui le réseau de l'opérateur 3G est terrain de chasse libre.

La différence quantitative entre le "*cracker*" de base dans son garage et une organisation étatique ou para-étatique devient en outre une différence qualitative. Le fait de pouvoir tout observer rend l'inférence beaucoup plus efficace, même en cas de chiffrement. Ainsi, un observateur présent en beaucoup d'endroits peut corréler des flux réseau entre eux, même s'ils sont chiffrés. Un observateur présent en un seul point du réseau n'a pas cette possibilité. Un simple VPN chiffré peut le rendre aveugle, alors que l'observateur présent partout peut trouver les serveurs où on se connecte uniquement en corrélant le trafic du VPN avec le trafic simultané en un autre point de l'Internet (XKEYSCORE fait apparemment cela.)

En prime, les attaquants susceptibles de monter un système de surveillance massive, comme la DGSE, sont également souvent capables de subvertir l'authentification. Chiffrer, en effet, ne sert pas beaucoup si on chiffre, non pas pour le vrai destinataire mais pour l'homme du milieu. La protection habituelle contre ces attaques de l'homme du milieu est l'authentification. Par exemple, on vérifie l'identité du correspondant via un certificat X.509. Mais une organisation puissante peut contraindre les autorités de certification à émettre de vrais/faux certificats <http://www.01net.com/actualites/comment-le-ministere-des-finances-espionne-le-trafic-web-de-ses-collaborateurs-610140.html>. Comme il suffit d'**une seule** autorité de certification contrainte (ou piratée, ce qui revient au même) pour faire un certificat pour n'importe quel serveur, on voit que la NSA n'a que l'embarras du choix.

Tout cela ne veut pas forcément dire qu'un attaquant puissant comme la NSA ou le FSB a table ouverte. Ces attaques ont des **coûts** et l'analyse de ces coûts est une branche relativement récente de la sécurité (elle est bien illustrée dans un excellent dessin de XKCD <https://xkcd.com/538/>). On ne peut évidemment pas espérer aveugler les agences d'espionnage mais on peut augmenter le prix de leurs activités, jusqu'à les forcer à réduire ces activités. La section 5.2 de notre RFC discute ces coûts.

Tous ne sont pas forcément monétaires. Par exemple, comme les espions, à l'égal des cloportes, n'aiment pas la lumière, le risque d'être pris la main dans le sac, représente un coût. Cela suppose évidemment que l'espion soit détecté et identifié. Si c'est fait, les conséquences peuvent aller de la fermeture d'une voie d'accès aux données, à des poursuites judiciaires, ou à la démission d'un ministre bouc émissaire.

Par exemple, une attaque passive offre à priori moins de chance de se faire attraper puisqu'on ne modifie pas le trafic. Sauf qu'un branchement physique sur des câbles va laisser des traces (les plombiers du Watergate ou du Canard Enchainé en savent quelque chose). Si l'opérateur réseau n'est pas complice de l'attaquant (il semble que, dans le cas de TEMPORA, il l'était), la « bretelle » peut être découverte à l'occasion d'une opération de maintenance, comme ce fut le cas dans l'affaire de Tarnac. Même si l'écoute se faisait de manière purement logicielle, un employé zélé peut la détecter un jour (« mais pourquoi ce port du commutateur est-il en mode miroir ? »). Les techniques sans-fil ne nécessitent pas de branchement physique mais, souvent, la portée utile est faible et l'attaquant doit se rapprocher, ce qui peut mener à sa détection. Bref, la vie d'un espion n'est pas toujours facile. Si l'opérateur collabore, c'est plus facile pour l'espion mais, s'il y a un Snowden parmi les employés de l'opérateur, patatras, la belle opération secrète d'écoute finit en une du Monde ou du New York Times. Si l'attaquant est un État, il peut forcer les employés d'un opérateur national à collaborer mais c'est plus difficile avec les étrangers.

C'est encore pire (du point de vue de l'attaquant) avec les méthodes actives. Elles laissent forcément davantage de traces. Par exemple, un vrai/faux certificat X.509 peut être détecté par des mesures comme les « certificats au grand jour » du RFC 6962.

Les attaques actives représentent aussi souvent un défi technique plus important. Là où les attaques passives nécessitent surtout des gros disques durs, les attaques actives peuvent demander, par exemple, qu'un injecteur de paquets frauduleux gagne la course contre la source légitime afin que ses paquets arrivent avant. À un térabit/s, ce n'est pas évident et cela ne se fait pas avec un PC ordinaire !

Voilà, on a fait un tour partiel des attaquants et de leurs capacités. Les solutions à ces attaques seront développées plus tard (mais cela ne sera pas facile).