RFC 8065 : Privacy Considerations for IPv6 Adaptation-Layer Mechanisms

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 février 2017

Date de publication du RFC : Février 2017

https://www.bortzmeyer.org/8065.html

Entre la couche 3 (du modèle en couches) et la couche 2 (par exemple Ethernet) se trouve une **adaptation**, qui définit comment on va mettre les paquets IPv6 sur la couche sous-jacente. Certaines de ces adaptations posent des problèmes de protection de la vie privée. Ce RFC résume les problèmes existants. Chaque adaptation devra ensuite travailler à s'améliorer sur ce plan (le RFC donne des idées). L'idée est d'améliorer les normes actuelles et futures, pour mieux prendre en compte ce problème de vie privée.

Ce problème de la vie privée pour IPv6 a déjà été beaucoup discuté, notamment en raison d'un choix initial de privilégier une adaptation à Ethernet qui gardait une partie de l'adresse IPv6 constante, même quand la machine changeait de réseau. Ce problème est résolu depuis longtemps (RFC 8981 [1]) mais d'autres peuvent demeurer, surtout si la couche 2 a des contraintes qui empêchent de déployer certaines protections de la vie privée.

Les documents de référence à lire d'abord sont le RFC général sur la vie privée, RFC 6973 (sa section 5.2 est particulièrement utile ici), et, plus spécifique à IPv6, le RFC 7721. Le risque qui concerne l'adaptation est lié au mécanisme de génération des IID (identificateurs d'interface, cf. RFC 4291), puisque cet IID fait partie de l'adresse IPv6 (typiquement les 64 derniers bits) et va donc être potentiellement visible publiquement. Si l'IID est trop prévisible ou trop stable, il permettra notamment :

— De corréler des activités du même utilisateur au cours du temps,
— De suivre l'utilisateur à la trace s'il se déplace en gardant le même IID,
— De balayer plus facilement un réseau à la recherche de machines à attaquer (alors que, normalement, la taille élevée de l'espace d'adressage IPv6 rend ces balayages lents et pénibles).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8981.txt

Un concept important est celui d'**entropie**, c'est-à-dire du nombre de bits dans l'IID qui sont réellement imprévisibles. Idéalement, l'entropie devrait être de 64 bits (le préfixe IPv6 ayant typiquement une longueur de 64 bits pour un réseau, cf. RFC 7421).

Voilà pourquoi le RFC 8064 déconseille de créer un IID à partir d'une adresse « couche 2 » fixe, comme l'est souvent l'adresse MAC. Il recommande au contraire la technique du RFC 7217 si on veut des adresses stables tant qu'on ne se déplace pas, et celle du RFC 8981 si on veut être vraiment difficile à tracer (au prix d'une administration réseaux plus difficile). Le RFC sur la sélection des adresses source, RFC 6724 privilégie déjà par défaut les adresses temporaires du RFC 8981.

Revenons maintenant à cette histoire d'entropie (section 2 du RFC). Combien de bits sont-ils nécessaires ? Prenons le cas le plus difficile, celui d'un balayage du réseau local, avec des paquets ICMP "*Echo Request*" ou bien avec des TCP `SYN`. L'entropie minimum est celle qui minimise les chances d'un attaquant de trouver une adresse qui réponde. Quel temps faudra-t-il pour avoir une chance sur deux de trouver une adresse ? (Notez que la capacité de l'attaquant à trouver des machines dépend aussi du fait qu'elles répondent ou pas. Si une machine ne répond pas aux ICMP "*Echo Request*", et n'envoie pas de `RST` aux paquets TCP `SYN`, la tâche de l'attaquant sera plus compliquée. Cf. RFC 7288, notamment sa section 5. Même si la machine répond, un limiteur de trafic peut rendre la tâche de l'attaquant pénible. Avec la valeur par défaut d'IOS de deux réponses ICMP par seconde, il faut une année pour balayer un espace de seulement 26 bits.)

Les formules mathématiques détaillées sont dans cette section 2 du RFC. L'entropie nécessaire dépend de la taille de l'espace d'adressage mais aussi de la durée de vie du réseau. Avec $2\hat{\}16$ machines sur le réseau (c'est un grand réseau !) et un réseau qui fonctionne pendant 8 ans, il faudra 46 bits d'entropie pour que l'attaquant n'ait qu'une chance sur deux de trouver une machine qui réponde (avec la même limite de 2 requêtes par seconde ; sinon, il faudra davantage d'entropie).

Et combien de bits d'entropie a-t-on avec les techniques actuelles ? La section 3 donne quelques exemples : seulement 48 bits en Bluetooth (RFC 7668), 8 (oui, uniquement 256 adresses possibles, mais c'est nécessaire pour permettre la compression des en-têtes) en G.9959 (RFC 7428) et le pire, 5 bits pour NFC (RFC pas encore paru).

Ces adaptations d'IPv6 à diverses couches 2 utilisent comme identificants d'interface des adresses IEEE (comme les adresses MAC) ou bien des « adresses courtes ». Commençons par les adresses reposant sur des adresses IEEE. Dans certains cas, la carte ou la puce qui gère le réseau dispose d'une adresse EUI-48 ou EUI-64 (comme l'adresse MAC des cartes Ethernet). On peut facilement construire une adresse IPv6 avec ces adresses, en concaténant le préfixe avec cette adresse IEEE utilisée comme identificateur d'interface (IID). L'entropie dépend du caractère imprévisible de l'adresse IEEE. L'IEEE a d'ailleurs des mécanismes `<https://mentor.ieee.org/privecsg/documents>` (pas forcément déployés dans le vrai monde) pour rendre ces adresses imprévisibles. Même dans ce cas, la corrélation temporelle reste possible, sauf si on change les adresses de temps en temps (par exemple avec macchanger `<http://www.gnu.org/software/macchanger>`).

Un argument souvent donné en faveur des adresses MAC est leur unicité, qui garantit que les adresses IPv6 seront « automatiquement » distinctes, rendant ainsi inutile la détection d'adresses dupliquées (DAD, RFC 4862, section 5.4, et RFC 4429, annexe A). Sauf que ce n'est pas vrai, les adresses MAC ne sont pas forcément uniques, en pratique et les identificateurs d'interface aléatoires sont donc préférables, pour éviter les collisions d'adresses.

En dehors des adresses allouées par un mécanismes de l'IEEE, il y a les « adresses courtes » (16 bits, utilisées par IEEE 802.15.4, cf. RFC 4944), allouées localement, et uniques seulement à l'intérieur du

réseau local. Vu leur taille, elles n'offrent évidemment pas assez d'entropie. Il faut donc les étendre avant de s'en servir comme identificateur d'interface. Le RFC cite par exemple un condensat de la concaténation de l'adresse courte avec un secret partagé par toutes les machines du réseau.

On peut aussi utiliser dans le condensat le numéro de version spécifié dans la section 4.3 du RFC 6775. Ainsi, un changement de numéro de version permettra une rénumérotation automatique.

Bien, après cette analyse, les recommandations (section 4) :

— La section Sécurité ("*Security Considerations*") des RFC qui normalisent une adaptation à une couche 2 donnée devrait dire clairement comment on limite le balayage. Cela nécessite de préciser clairement la durée de vie des adresses, et le nombre de bits d'entropie.
— Il faut évidemment essayer de maximiser cette entropie. Avoir des identificateurs d'adresses aléatoires est une bonne façon de le faire.
— En tout cas, pas question de juste utiliser une adresse courte et stable avec quelques bits supplémentaires de valeur fixe et bien connue.
— Les adresses ne devraient pas être éternelles, pour limiter la durée des corrélations temporelles.
— Si une machine peut se déplacer d'un réseau à l'autre (ce qui est courant aujourd'hui), il faudrait que l'identifiant d'interface change, pour limiter les corrélations spatiales.