IPv6 ET VIE PRIVÉE

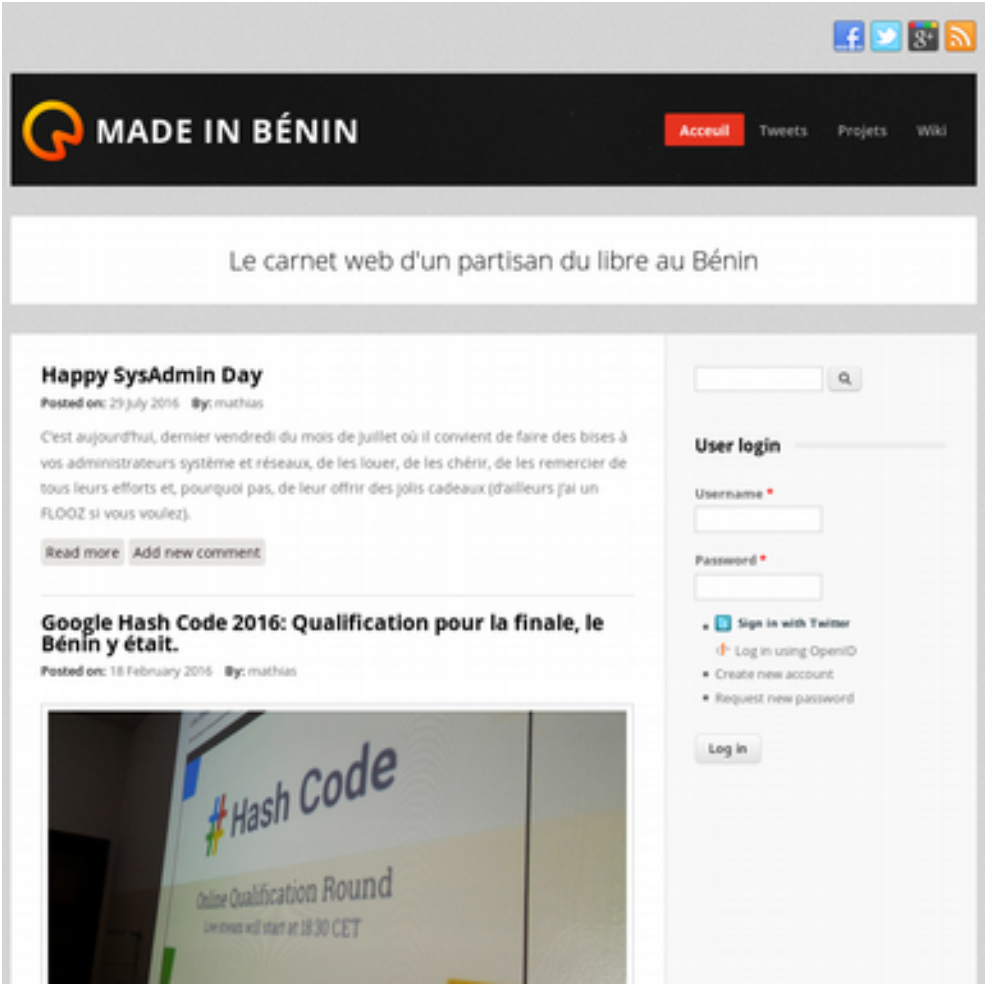
15 octobre 2016

IGB@NET
www.igbanet.org

A propos de moi

Où me trouver sur Internet ?

- Blog http://mathias.houngbo.net
- Twitter @mhoungbo
- AdminSys le jour, Développeur la nuit, Enseignant occasionnellement.



Pourquoi cette présentation ?

Pourquoi cette présentation ?

Le futur d'Internet est l'adressage IPv6 en lieu et place de l'actuel protocole IPv4, puisque nous sommes en train d'atteindre les limites de ce dernier.

Pourquoi cette présentation ?

Malgré ses indéniables atouts, le protocole IPv6 pose certaines questions sur le respect de la vie privée lors de sa configuration automatique. Nous proposons dans cette présentation de passer en revue les problèmes et d'esquisser des solutions afin de mieux protéger sa vie privée avec IPv6.

Pourquoi cette présentation ?

- il n'y a plus besoin de créer des réseaux « privés » (avec un NAT) puisque le nombre d'adresses disponibles est largement suffisant. Ainsi, si les règles de routage le permettent, les clients peuvent être connectés directement entre eux (ce qui facilite l'adoption des connexions P2P). Ne pas avoir à configurer de NAT est un grand avantage également pour l'auto-hébergement, car il n'y a pas besoin de gérer l'ouverture et la redirection des ports du routeur, ce qui simplifie grandement sa configuration, puisque "seul" le pare-feu doit être géré ;
- il n'y a plus de nécessité de coordinateur central pour gérer les baux d'adresses d'un sous-réseau (DHCP), puisqu'il suffit de tester si une adresse tirée au hasard est disponible, tester si quelqu'un l'utilise et l'utiliser (ou tester une nouvelle) ;

Pourquoi cette présentation ?

- les cartes réseau peuvent louer autant d'adresses que désiré, puisque les sous-réseaux contiennent suffisamment d'adresses disponibles (bien plus que les fameuses 255 adresses fournies par les réseaux privés installés par défaut) ;
- le routeur est capable de s'annoncer directement sur le réseau pour tous les appareils lui étant connectés par le réseau « lien-local » (i.e. physiquement branché sur le même réseau). Ainsi, les clients peuvent se configurer automatiquement pour avoir accès au reste d'Internet. Ceci est possible grâce à la possibilité d'avoir plusieurs adresses par interface : une adresse lien-local utilisée pour recevoir les informations et mises à jour du réseau local et une adresse globale pour se connecter au reste d'Internet.

Pourquoi cette présentation ?

Malgré tous ces avantages, un des inconvénients connus d'IPv6 est que le fichage du trafic des ordinateurs particuliers est plus aisé par les attaquants. En effet, une des propriétés du protocole NAT était d'utiliser une seule adresse IPv4 publique pour plusieurs appareils, ce qui rendait un peu plus difficile le fichage des utilisateurs, puisque plusieurs d'entre eux utilisaient la même adresse pour se connecter à Internet.

Avec IPv6, chaque ordinateur ayant sa propre adresse publique, l'attaquant peut faire un lien direct entre une adresse et un utilisateur particulier.

Pourquoi cette présentation ?

Un attaquant pourrait être un homme du milieu qui écouterait le trafic IP ou une personne ayant accès à des logs de différents serveurs. Avec de telles informations, l'attaquant pourrait faire des liens entre les différentes activités des utilisateurs, bien qu'elles ne soient pas liées directement.

Par exemple, il pourrait savoir quand un employé travaille sur Internet ou quand une personne est présente chez elle.

Il faudrait donc veiller à ce que les machines du réseau changent d'adresse IP publique régulièrement pour rendre le fichage plus difficile. Il pourrait changer à travers le temps et/ou selon le réseau auquel il se connecte.

Connexion aux réseaux en IPv6 avec l'autoconfiguration

Connexion aux réseaux en IPv6 avec l'autoconfiguration

Pour commencer, il faut savoir que les adresses IPv6 sont définies en deux parties :

- **le préfixe réseau qui est défini par le FAI. Il est annoncé sur le réseau par le routeur au moyen des adresses de type lien-local.**

- **l'identifiant d'interface qui se compose des bits restants et qui identifie une interface d'une machine dans le réseau.**

RFC 4941 : rendre les adresses auto-configurées temporaires

Rendre les adresses auto-configurées temporaires

Cet RFC propose de rendre le pistage du trafic d'un client IPv6 plus difficile en étendant la définition des types d'adresses IPv6 avec un type temporaire.

Il propose une solution pour résoudre les problèmes suivants :

- Comme l'identifiant d'interface reste constant à travers tous les réseaux auxquels le client se connecte, un attaquant, qui aurait accès aux logs de différents serveurs, peut trouver des corrélations entre les différentes activités du client.
- Un attaquant qui écouterait le trafic du réseau peut facilement retrouver les communications d'un client précis en lisant les données IPv6 des paquets réseau.

Rendre les adresses auto-configurées temporaires

Pour résoudre les problèmes identifiés, le RFC propose de créer le principe de type d'adresse « temporaire », c'est-à-dire des adresses qui auront l'obligation de passer à un statut obsolète après un certain temps et qui ne seront pas devinables en utilisant des informations disponibles sur le réseau.

Ce RFC précise donc un algorithme qui remplacera l'utilisation de l'adresse MAC pour trouver rapidement un identifiant unique par l'utilisation du hasard. Il conserve les autres principes de l'auto-configuration, mais permet de créer directement un ensemble d'adresses temporaires (au lieu d'une seule adresse) et détermine une période de regénération et remplacement de ces adresses.

RFC 7217 : créer par défaut des identifiants d'interface non-prédictibles et stables

Créer par défaut des identifiants d'interface non-prédictibles et stables

Le RFC précédent définit les adresses temporaires pour des communications sortantes, mais elles nécessitent toujours les adresses IP crées avec les adresses MAC pour l'établissement des communications entrantes (fonctionnalités de type serveur).

Le RFC 7217 propose une solution pour rendre plus opaques ces adresses stables nécessaires aux fonctions de type serveur. En effet, l'utilisation de l'adresse MAC permet encore à un attaquant de trouver des corrélations d'activités sur Internet et il peut également plus facilement réduire le nombre d'adresses en cours d'utilisation à scanner (puisque l'adresse MAC réduit le nombre d'identifiants possibles, notamment en connaissant le constructeur des interfaces réseau).

Créer par défaut des identifiants d'interface non-prédictibles et stables

Dans les grandes lignes, l'algorithme produit des identifiants d'interface stables pour un réseau donné. C'est à dire qu'à chaque changement de réseau, les identifiants changent, mais lors du retour sur un réseau, il devrait reprendre la même valeur qu'auparavant (si l'identifiant n'a pas été utilisé par un autre appareil entre temps). Malgré cette stabilité, les identifiants ne sont pas prédictibles, car l'algorithme utilise une clé privée connue uniquement par le système local.

Conclusion

Conclusion

Finalement, avec l'activation de ces 2 RFCs dans les gestionnaires de réseau des machines, il est possible d'avoir les avantages de l'auto-configuration d'IPv6 avec une protection de la vie privée au moins égale à celle de l'utilisation d'un NAT avec IPv4.

En effet, le RFC 7217 permet de toujours créer des adresses non-prédictibles (et différentes sur chaque réseau) et le RFC 4941 permet de créer des adresses temporaires qui auront l'obligation d'être abandonnées après un certain temps d'utilisation.

Le travail des attaquants est donc rendu bien plus difficile pour créer des corrélations des activités d'une machine sur les réseaux tout en gardant l'avantage d'IPv6 où la configuration manuelle n'est pas nécessaire et où les adresses IPs utilisées sur le réseau sont toutes des adresses publiques facilitant le P2P.

Merci de votre attention
Place aux questions.

« Mefies toi de la médiocrité, c'est la moisissure de l'esprit »