DNSSEC

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

25 juin 2010

Nous allons tous mourir !

(Exposé de Rod Beckstrom, directeur de l'ICANN, à la réunion de Nairobi en mars 2010.) « *The DNS is more fragile than it has ever been and it could stop at any time. . . . As CEO of ICANN I met with heads of security for the 3 largest countries in the world and they are concerned.* »

Nous allons tous mourir !

(Exposé de Rod Beckstrom, directeur de l'ICANN, à la réunion de Nairobi en mars 2010.) « *The DNS is more fragile than it has ever been and it could stop at any time. . . . As CEO of ICANN I met with heads of security for the 3 largest countries in the world and they are concerned.* »

Info ou intox ? Par delà son désir de « vendre » le projet de DNS-CERT, il faut bien constater que les problèmes existent.

L'écosystème du DNS

Une résolution DNS complète et authentique dépend :

1. De la chaîne d'enregistrement (du titulaire du nom au registre),
2. De la chaîne de résolution (du registre à l'utilisateur)

L'écosystème du DNS

Une résolution DNS complète et authentique dépend :

1. De la chaîne d'enregistrement (du titulaire du nom au registre),
2. De la chaîne de résolution (du registre à l'utilisateur)

Et il y a tout ce qui n'est pas le DNS mais est néanmoins indispensable à l'utilisation de l'Internet (risques BGP, machines Windows zombies, ...).

La chaîne de résolution

1. Registre -> Serveurs faisant autorité
2. Serveurs faisant autorité -> Résolveur
3. Titulaire ou BE -> Hébergeur DNS
4. Résolveur -> Utilisateur final

La chaîne de résolution

1. Registre -> Serveurs faisant autorité
2. Serveurs faisant autorité -> Résolveur
3. Titulaire ou BE -> Hébergeur DNS
4. Résolveur -> Utilisateur final

Chaque étape a ses attaques possibles (usurpation du serveur maître, attaque Kaminsky, résolveurs menteurs, ingéniérie sociale, écoute du réseau et des mots de passe).

Principe d'une attaque Kaminsky

Mallory veut empoisonner le serveur Alice

1. Mallory suscite une question DNS **pour un nom non-existant**, envoyée par Alice au serveur faisant autorité Bob
2. Mallory répond avant Bob, en devinant le *cookie* (*Query ID* sur 16 bits)
3. Alice accepte la réponse
4. Si ça rate, Mallory essaie encore

Le DNS dans la tempête

RFC 3833 *Threat Analysis of the Domain Name System*

RFC 5452 *Measures for Making DNS More Resilient against Forged Answers* : un manuel très concret du fraudeur. À 100 Mb/s, empoisonnement réussi en quelques jours (expérience faite par nos collègues tchèques)

Principes de DNSSEC

Signature cryptographique des enregistrements DNS : **sécurité de bout en bout**.

Normalisé depuis des années. Mis en œuvre dans tous les logiciels. Largement déployé dans les TLD (mais pas dans les sous-domaines). Mais pas dans les résolveurs des FAI.

Everybody loves screenshots

```
% dig +dnssec A ripe.net.
...
;; ANSWER SECTION:
ripe.net.                600     IN      A       193.0.0.214
ripe.net.                600     IN      RRSIG   A 5 2 600 \
        20101221061607 20101121061607 49526 ripe.net. \
        2NePKf/On6ZgcQDOzpinEou4QiojhW1A2IKoxHBdtawMa7aSeQdL+hZ
```

Je signe mes zones

BIND, ldns, logiciels privateurs...

Le plus dur est la gestion des clés. OpenDNSSEC permet de l'automatiser.

La taille compte

Attention, les réponses DNS sont plus grosses : on dépasse souvent l'antédiluvienne limite de 512 octets.

Si vous avez encore des pare-feux qui limitent à 512, il est temps d'agir. (Cela a sans doute déjà planté avec la signature de la racine.)

Rôle de l'AFNIC

1. Rôle direct : choix des serveurs, bonnes pratiques en matière de sécurité, déploiement de DNSSEC
2. Rôle indirect : sensibilisation de la communauté, encouragement aux BE à auditer leur code, information et formation, normalisation, partage d'informations (DNS-OARC et autres forums).

Actions indirectes

Sensibilisation

- Animation de la liste francophone sur le DNS, `dns-fr@cru.fr`,
- Communication en direction des BE (listes comme `fai@afnic.fr`)
- Dossier thématique « DNS : types d'attaques et techniques de sécurisation » `http://www.afnic.fr/actu/nouvelles/224/l-afnic-publie-un-nouveau-dossier-thematic`

DNSSEC dans .FR

Pour faire face aux risques de modification des données (attaque Kaminsky) :

1. Signature de la zone "`fr`" le 14 septembre 2010
2. Délégations sécurisées en 2011

Les signatures utiliseront RSA (2048 bits) et SHA-256. La zone sera signée avec NSEC3 et *opt-out*.

DNSSEC dans la racine

1. Signature de la zone racine déjà faite
2. Délégations sécurisées déjà faites (“.uk”, “.cz”, “.br”)
3. Publication de la clé le 15 juillet

Place aux trolls

Place aux trolls

1. Combien ça va coûter ? Qui va payer ?

Place aux trolls

1. Combien ça va coûter ? Qui va payer ?
2. Il n'y a pas de problème plus urgent ? La sécurité de BGP ?

Place aux trolls

1. Combien ça va coûter ? Qui va payer ?
2. Il n'y a pas de problème plus urgent ? La sécurité de BGP ?
3. C'est bien compliqué.

Place aux trolls

1. Combien ça va coûter ? Qui va payer ?
2. Il n'y a pas de problème plus urgent ? La sécurité de BGP ?
3. C'est bien compliqué.
4. Si même "`.arpa`" et "`.gov`" se plantent, qui va y arriver ?

Place aux trolls

1. Combien ça va coûter ? Qui va payer ?
2. Il n'y a pas de problème plus urgent ? La sécurité de BGP ?
3. C'est bien compliqué.
4. Si même "`.arpa`" et "`.gov`" se plantent, qui va y arriver ?
5. La cryptographie, ça plante plus souvent que ça ne protège.