Jean Saquet – Université de Caen

Master d'Informatique – e-secure

Réseaux

DNSSEC

Bureau S3-354
Mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M2

DNS : rappel du principe

Base de données répartie et hiérarchique
Contient les associations entre noms de domaine et informations telles que adresses IP, serveurs de courrier, de nom, …
Informations contenues dans les RRs, eux même situés dans des fichiers de zone ou reverse.

Protocole pour l'interrogation des serveurs, et pour l'échange d'information entre serveurs.

DNS : vulnérabilités

Le DNS est essentiel au fonctionnement de l'Internet :
- pbs en cas de dénis de service
- besoin de disponibilité permanente
- problème d'authenticité et d'intégrité des données

Risque de falsification des données au niveau des fichiers (cas de mise à jour dynamique) ou lors de la transmission entre serveurs, ou entre client et serveur.

DNS : but des attaques

- Blocage du service

- Redirection des utilisateurs,
en vue d'attaques plus graves

- Récupération d'informations confidentielles
(ex. : courrier)

- ...

DNSSEC : principes

But : sécuriser les données

Besoin : essentiellement signature (données publiques)

Moyens :
outils cryptographiques,
clés d'authentification (symétriques ou non),
avec architecture de distribution de clés

DNS : besoins spécifiques

Sécurité du transfert de zones
(entre serveur primaire et secondaires)

Mises à jour dynamiques

Lien entre client et serveur le plus proche

Tout ceci peut se faire en dehors de DNSSEC,
Des solutions ont été proposées.

Transaction SIGnature

Technique proposée pour la liaison maître / secondaire :

Clé secrète partagée, générée par le maître, transmise aux secondaires « manuellement »

Assure authenticité et intégrité des échanges
Protection contre le rejeu possible par utilisation d'un datage.

Utilisation d'IPSEC ?

On pourrait établir des associations de sécurité entre serveur maître et esclaves, entre serveur et client pouvant mettre à jour dynamiquement.

Mais il faut une association par paire, peu pratique, lourd à gérer.

DNSSEC

Version 1 : 1999

DNSSEC bis : 2005

NSEC3 : mars 2008

Implémenté dans Bind et autres logiciels.

Extensions DNSSEC

Besoins :

- Signer les données envoyées
- Prouver la non-existence d'une donnée
- Vérifier authenticité et intégrité des données

Doit régler aussi le pb de la distribution de clés.

DNSSEC côté serveur

Chaque zone génère une ou des paires de clés.

Ces clés sont associées à la zone, pas au serveur

La clef privée signe les infos sur lequel le serveur a autorité.

Tout ceci doit rester compatible avec le DNS d'origine.

DNSSEC nouveaux RRs

DNSKEY stocke la clef publique

RRSIG stocke la signature d'une donnée signée par la clef privée correspondant à DNSKEY

Ces données sont lisibles.
Bien entendu, la clef secrète n'est pas dans la base lisible

La syntaxe est conforme à celle des autres RRs, la partie donnée étant spécifique pour chaque RR.

DNSSEC réponses négatives

Problème : signer l'absence de réponse
Une « non-réponse » n'est pas basée sur un RR, donc on ne peut pas signer ce dernier !

Principe de la solution : les enregistrements NSEC relatifs aux données du domaine sont organisés en liste chaînée circulaire, basée sur les noms des ressources.
Si une donnée n'existe pas, le serveur renvoie un RR signé avec des infos existantes, celles qui encadrent au sens ordre ASCII) l'enregistrement inexistant.

DNSSEC pb de « walk »

La gestion des non réponses peut provoquer la possibilité de récupérer tous les RRs de la zone.
(parcours de zone ou DNS walking)

NSEC3 résout le problème en chaînant sur les hachages des noms au lieu des noms.

DNSSEC côté client

La connaissance de la clé publique permet de vérifier les signatures.

Reste, comme toujours, à faire confiance à cette clé publique …

Une « clé de confiance » doit être configurée statiquement, permettant d'établir un point de départ d'une chaîne de confiance.

DNSSEC chaînes de confiance

Délégation sécurisée : la zone parente authentifie la clé publique de la zone fille.

Une chaîne de confiance est un chemin connexe dans l'arbre des délégations DNS, où chaque passage d'une zone parente à une zone fille est une délégation sécurisée.

Un record DS permet de signer et authentifier la clé d'une zone fille.
Une absence authentifiée de DS indique qu'une telle délégation sécurisée n'existe pas.

DNSSEC but, état

Une zone peut ainsi être non sécurisée, localement sécurisée (signature locale mais la délégation depuis la zone parente n'est pas sécurisée), ou sécurisée globalement depuis une zone de confiance.

L'arbre DNS est constitué d'ilôts sécurisés et d'autres non. Le but de DNSSEC serait de sécuriser l'ensemble

DNSSEC DLV

Dnssec Lookaside Validation sépare la racine du DNS de celle de validation.

Le résolveur DLV demande à une racine DLV de valider la chaîne.
Un domaine signé, ou au moins le début d'un chemin de confiance vers ce domaine, sera signalé dans un record DLV sur cette racine.

Exemple : registre DLV chez ISC (Internet Systems Consortium).
Pas utile si la racine est signée.

DNSSEC durée de vie des clés

Des clés courtes doivent être renouvelées de temps en temps, ce qui peut être lourd pour les relations de délégation sécurisée.

En pratique, on utilise des clés courtes pour signer les enregistrements d'une zone, et on la renouvelle fréquemment, mais on utilise des clés longues pour les maillons de confiance.

DNSSEC problèmes

Réponses plus longues (plus qu'un DG)

Lourdeur de mise en place

Nécessite des ressources complémentaires

Mais : BIND adapté, racine et de nombreux TLD signés.