Jean Saquet – Université de Caen

Master e-secure

Sécurité réseaux

CGA et SEND

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

Insuffisances de NDP

Le protocole Neighboor Discovery Protocol n'est pas sécurisé. Leurs auteurs avaient pensé qu'IPSEC aurait pu résoudre le problème, mais comment utiliser IPSEC avant d'avoir une configuration IP opérationnelle ?

Il est facile de prétendre posséder une adresse, ou de diffuser de fausses annonces de routeur (préfixes, routes, …)

L'autoconfiguration IPv6 peut donc facilement être perturbée.

Contraintes

Une machine affirmant qu'elle possède une adresse doit pouvoir prouver qu'elle a eu le droit de se l'approprier.

Ceci doit toutefois pouvoir se faire sans vérification de certificat dans une chaîne de confiance, car une telle adresse est présentée par une machine qui vient de se forger cette adresse et qui ne possède pas encore de configuration opérationnelle.

Un routeur par contre est censé posséder une telle configuration.

Principes (1)

L'adresse sera générée, par une méthode normalisée, à partir d'une paire de clés publique/privée et signée par cette dernière. Grâce à la clef publique, un partenaire pourra vérifier la validité de cette adresse.

Les routeurs pourront posséder un certificat et fournir aux machines la route d'accès vers les autorités de certification. Si la vérification fonctionne, la machine pourra alors utiliser en confiance les informations fournies par le routeur.

Principes (2)

La machine désirant se forger une adresse CGA devra le faire selon un algorithme précis et en construisant une structure des paramètres associés.

Le protocole de détection d'adresse dupliquée sera modifié pour transporter les infos nécessaires à la vérification par les partenaires (envoi des paramètres et signature avec la clé privée).

Adresse CGA

Voir les documents annexes pour :
- La structure de données des paramètres
- L'algorithme de génération d'adresse CGA
- L'algorithme de vérification d'une adresse CGA

Un exemple de calcul est fourni dans le livre sur IPv6 de Gisèle Cizeault

SEND

SEND consiste en fait en un ajout d'options aux messages NDP, et bien sûr leur traitement.

Ces options sont :

- CGA : transporte les données publiques liées à l'adresse
- Signature : pour signer les données avec la clé privée
- Nonce : valeur aléatoire, et
- Horodatage : transport de l'heure, pour éviter le rejeu.

Il y a également des nouveaux messages.

SEND - utilisation

Les machines peuvent vérifier les adresses annoncées. Ainsi, toute tentative d'usurpation d'adresse sera détectée. L'option CGA permet de récupérer la clé publique de l'émetteur et l'option signature de la vérifier.

L'attaquant ne pourra donc pas forger un message valide à la place d'une machine qui est la seule à pouvoir prouver son adresse.

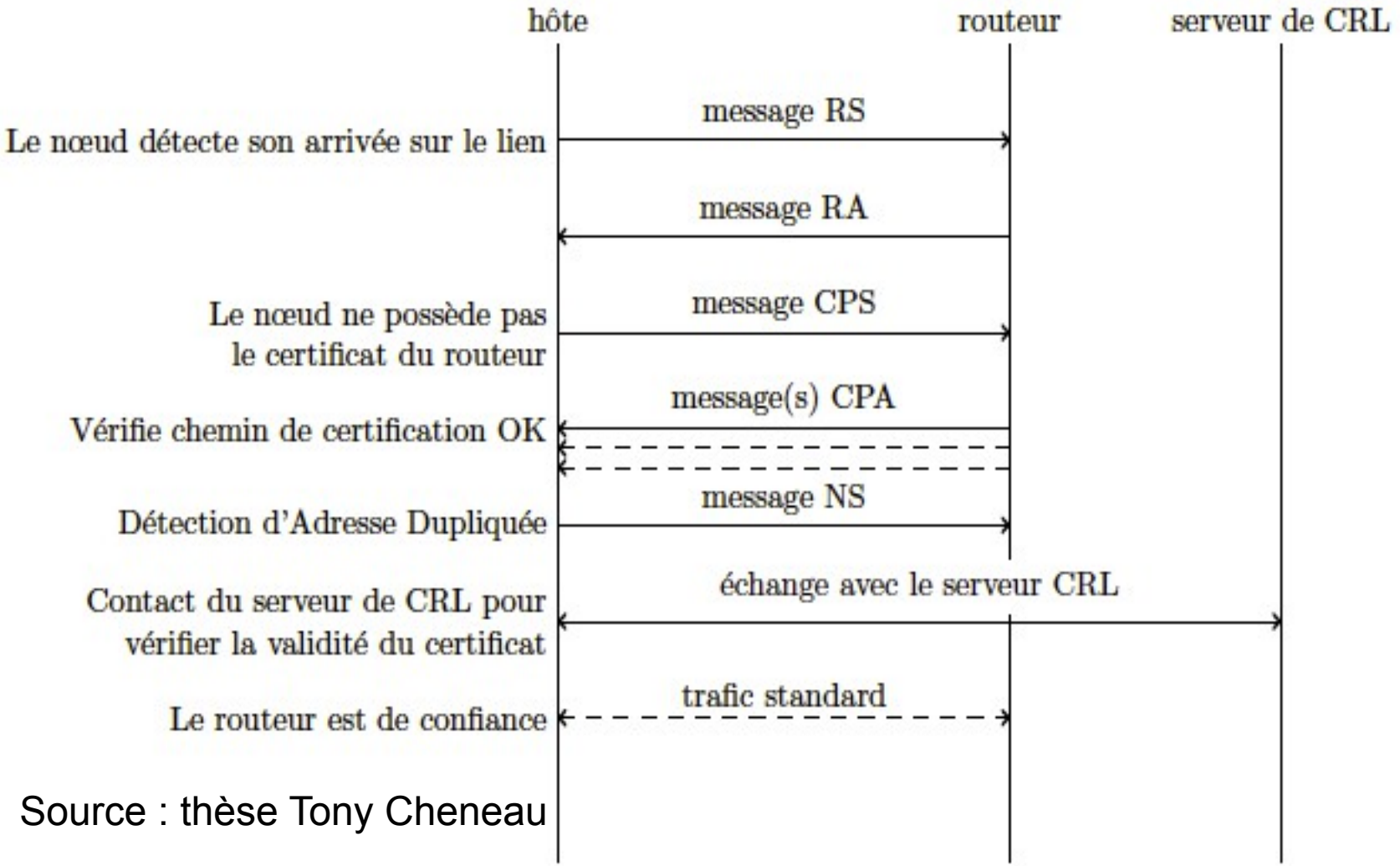
SEND - routeurs

Prouver son adresse ne suffit pas (voire n'apporte rien) pour les routeurs. Ceux-ci doivent justifier leur rôle pour prouver qu'ils ont le droit d'annoncer préfixes et routes.

SEND prévoit un message CPS pour découvrir le chemin de certification du routeur et un message CPA pour que le routeur puisse l'indiquer.

La machine qui reçoit les annonces de routeur peut alors vérifier l'authenticité du routeur avant de valider définitivement les infos de ce dernier.

NDP-SEND



Source : thèse Tony Cheneau

Transition

Le mécanisme CGA-SEND ne sera pas disponible du jour au lendemain sur tous les systèmes.
Il est prévu une phase de transition dans laquelle cohabitent le mécanisme NDP simple et CGA/SEND.

Mode mixte : les machines sécurisées peuvent accepter les annonces des autres machines, sous réserve de compatibilité avec les données reçues en mode sécurisé. Une donnée non sécurisée ne peut pas écraser une donnée obtenue en mode sécurisé.

SEND : limitations

Incompatibilité avec le mécanisme de mobilité car l'agent-mère doit répondre par procuration aux sollicitations du nœud mobile. Un mécanisme de NDP-proxy est également incompatible.

Incompatibilité avec les adresses anycast.

Risque de vulnérabilité pour les adresses lien-local car 59 bits variables seulement sur l'adresse

SEND : Coût

Les calculs prennent du temps. La condition sur les bits à 0 de l'étape 3 (calcul de hash2) nécessite en moyenne 2^{16xSEC} itérations de la fonction de hachage. En pratique, on prend souvent SEC=1 (voire 0).

Le calcul de hash1 inclus le préfixe réseau, pas celui de hash2. En cas de changement de préfixe, seul le calcul de hash1 est à refaire.

SEND : implémentations ?

DoCoMo : n'est plus maintenu

ipv6-send-cga : université de Pekin Postes et Telecom (2009?)

NDProtector : avec ajouts de Tony Cheneau

Cisco : version pour les routeurs de ce constructeur.

Easy-SEND