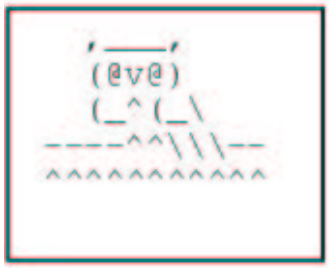

Projet RNRT

Infrastructure
DNS
sécurisée et
Applications

Sous-Projet 3

Livrable 3.4

Évaluation du service rendu par DNSSEC lors de son utilisation avec Mobile IPv6

Partenaire responsable: France Télécom R&D
Auteur(s): Gilles Guette, IRISA, (gguette@irisa.fr)
Date: 18/06/04
Version: 1.0
Contact: idsa-tech@nic.fr

Résumé/Abstract:
Le projet IDsA a déployé une plate-forme expérimentale basée sur une architecture DNS sécurisée grâce aux extensions DNSSEC et sur les technologies IPv6 et IPsec. Cette plateforme a pour buts de tester les implémentations DNSSEC, de fournir un cadre pour la création d'outils adaptés et d'étudier les applications possibles d'une telle architecture DNS sécurisée notamment pour la sécurisation du protocole Mobile IPv6.

IDsA project has deployed an experimental platform based on a secured DNS architecture (DNSSEC), and running on top of an IPv6/IPsec infrastructure. The goals of this platform are as follows: to test DNSSEC implementations, to be able to create and validate a set of tools and to study potential applications taking advantage of such a secured DNS architecture in particular securisation of Mobile IPv6 protocol.

1 Introduction

Actuellement, nous assistons à une évolution dans le monde de l'Internet, des réseaux et des services qui leurs sont associés. Nous assistons notamment à la diversification et à l'accroissement du nombre de machines mobiles ainsi qu'au besoin d'accéder à l'information de n'importe quel endroit. Intégrer le support de la mobilité dans les réseaux actuels est devenu une nécessité. Le protocole IPv6 inclut ce support, il est appelé Mobile IPv6 [JPA04, ADD04, HL01]. Mobile IPv6 (MIPv6) permet à un nœud mobile de se déplacer d'un lien à un autre sans changer son adresse IP mère. MIPv6 définit des messages de signalisation spécifiques afin qu'un nœud mobile reste toujours joignable par son adresse mère : l'adresse IP assignée au nœud mobile avec le préfixe de sous-réseau de son réseau d'origine. Ces messages de signalisation ne sont pas protégés et sont vulnérables à différentes attaques présentées dans la suite de ce document. La principale conséquence de ces attaques est de détourner le trafic en provenance ou à destination d'un nœud mobile. Dans ce document, nous présentons tout d'abord le protocole Mobile IPv6, puis les attaques contre ce protocole et nous terminons par une présentation des interactions possibles entre Mobile IPv6 et DNSSEC afin de lutter contre ces attaques.

2 Définitions

Le protocole Mobile IPv6 définit trois entités actives lors de l'établissement d'une communication :

- Le nœud mobile ou *Mobile Node*. La machine qui se déplace d'un sous-réseau à un autre.
- L'agent mère ou *Home Agent*. Un routeur du réseau d'origine du nœud mobile. C'est lui qui possède l'association entre l'adresse mère du nœud mobile et ses adresses temporaires dans les réseaux d'accueil.
- Le correspondant ou *Correspondent Node*. Une machine avec laquelle le nœud mobile échange des paquets.

Deux types d'adresses sont associés au nœud mobile :

- L'adresse mère du nœud mobile ou *Home Address*. L'adresse du nœud mobile lorsqu'il se trouve dans son réseau d'origine.
- Les adresses temporaires ou *Care-of Address*. Une adresse temporaire est une adresse unicast routable attribuée au nœud mobile lorsqu'il se trouve sur un autre réseau que son réseau d'origine.

Les associations entre l'adresse mère et les adresses temporaires d'un nœud mobile doivent être conservées dans une structure de données particulières :

- Le *Binding Cache*. La table d'association entre l'adresse mère d'un nœud mobile et ses adresses temporaires. Chaque correspondant et chaque agent mère possèdent un *Binding cache* afin de pouvoir communiquer avec un nœud mobile.

La signalisation MIPv6 nécessite des messages spécifiques :

- *Binding Update*. Le message envoyé par un nœud mobile à son agent mère ou à son correspondant pour l'informer de son adresse temporaire.
- *Binding Acknowledgement*. Le message envoyé par l'agent mère ou le correspondant au nœud mobile pour accuser la réception d'un message *Binding Update*.
- *Home Test Init Message* et *Care-of Test Init Message*. Ces messages sont utilisés par le mécanisme de *Return Routability* (*cf.* 4.2) et sont envoyés en même temps par le nœud mobile. Le premier message est envoyé à l'agent mère qui le relaye au correspondant et le second message est envoyé directement au correspondant.
- *Home Test Message*. C'est la réponse du correspondant au message *Home Test Init Message*. Cette réponse est envoyée à l'agent mère qui le relaie jusqu'au nœud mobile.
- *Care-of Test Message*. C'est la réponse du correspondant au message *Care-of Test Init Message*. Elle est envoyée directement au nœud mobile.

3 Présentation

Le protocole MIPv6 permet à un nœud mobile de se déplacer d'un sous-réseau à un autre tout en continuant à utiliser l'adresse mère pour identifier ce mobile. Un nœud mobile peut se trouver sur deux types

de réseaux, son réseau d'origine (*Home Network*) ou un réseau étranger (*Foreign Network*). Le nœud mobile possède une adresse mère qui lui est affectée en fonction du lien sur lequel il est connecté dans son réseau d'origine. Lorsque le nœud mobile se déplace sur un autre réseau que son réseau d'origine, il se voit attribuer une nouvelle adresse, il s'agit de son adresse temporaire courante. Après son déplacement d'un réseau à un autre, le nœud mobile dispose donc d'au moins deux adresses, son adresse mère et son adresse temporaire.

La figure 1 montre les messages de signalisation MIPv6 échangés entre un nœud mobile et son agent mère. Lorsque le nœud mobile arrive sur le réseau étranger, une adresse IPv6 lui est attribuée, cette adresse devient son adresse temporaire courante ①. Cette attribution d'adresse peut être réalisée lors de la phase de connexion du nœud mobile au réseau étranger à l'aide du protocole DHCP [Dro97]. Pour informer son agent mère de l'obtention de cette nouvelle adresse, le nœud mobile envoie à son agent mère un message *Binding Update* contenant cette nouvelle adresse ②. L'agent mère peut alors mettre à jour sa table d'association (*Binding Cache*) concernant le nœud mobile ③ et confirme la réception en envoyant un message *Binding Acknowledgement* ④.

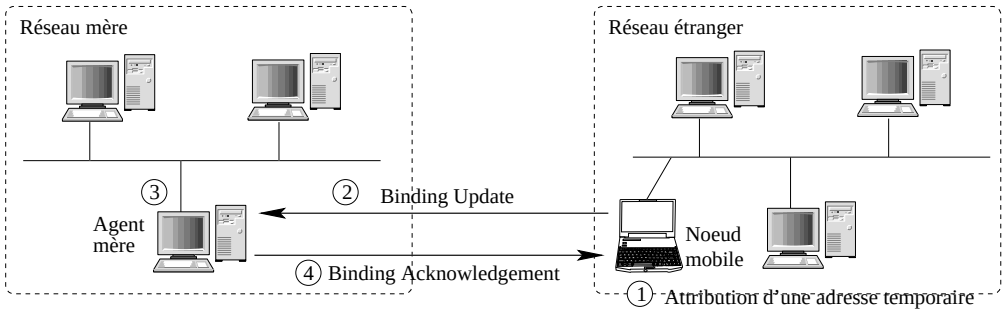

FIG. 1 – La signalisation MIPv6.

Un nœud mobile reste toujours joignable sur son adresse mère grâce à l'action de son agent mère. Lorsque le nœud mobile est connecté dans son réseau d'origine, les paquets à destination du nœud mobile sont routés normalement. Lorsque le nœud mobile se déplace sur un autre réseau, il existe 3 modes de transmissions possibles : le tunnel bidirectionnel, le routage triangulaire et le routage optimisé (*Route Optimization* ou RO).

3.1 Le tunnel bidirectionnel

Il s'agit de l'établissement d'un tunnel bidirectionnel entre le nœud mobile et son agent mère. Lors de l'établissement de ce tunnel bidirectionnel il y a authentification des deux parties communicantes.

La figure 2 montre l'acheminement des paquets entre un correspondant et le nœud mobile lorsqu'un tunnel est établi entre le nœud mobile et son agent mère. Lorsqu'un correspondant veut communiquer avec le nœud mobile, il envoie tous les paquets à destination de l'adresse mère du nœud mobile. Ces paquets sont interceptés par l'agent mère ① qui les tunnelle vers le nœud mobile ②. Les paquets envoyés par le nœud mobile au correspondant sont encapsulés dans des paquets à destination de l'agent mère ③ et c'est l'agent mère qui fait suivre ces paquets au correspondant ④.

3.2 Le routage triangulaire

La figure 3 décrit le principe du routage triangulaire quand le nœud mobile se trouve sur un réseau étranger.

Lorsque le correspondant veut communiquer avec le nœud mobile il envoie ses paquets à l'adresse mère du nœud mobile ①. Ces paquets arrivent à l'agent mère, celui-ci regarde dans sa table d'association (*Binding Cache*) s'il y a une entrée qui correspond à cette adresse primaire. Si oui il retransmet le paquet vers l'adresse temporaire du nœud mobile ②. Le nœud mobile, quant à lui, répond directement à l'adresse source contenue dans le message d'origine, c'est-à-dire l'adresse de son correspondant ③.

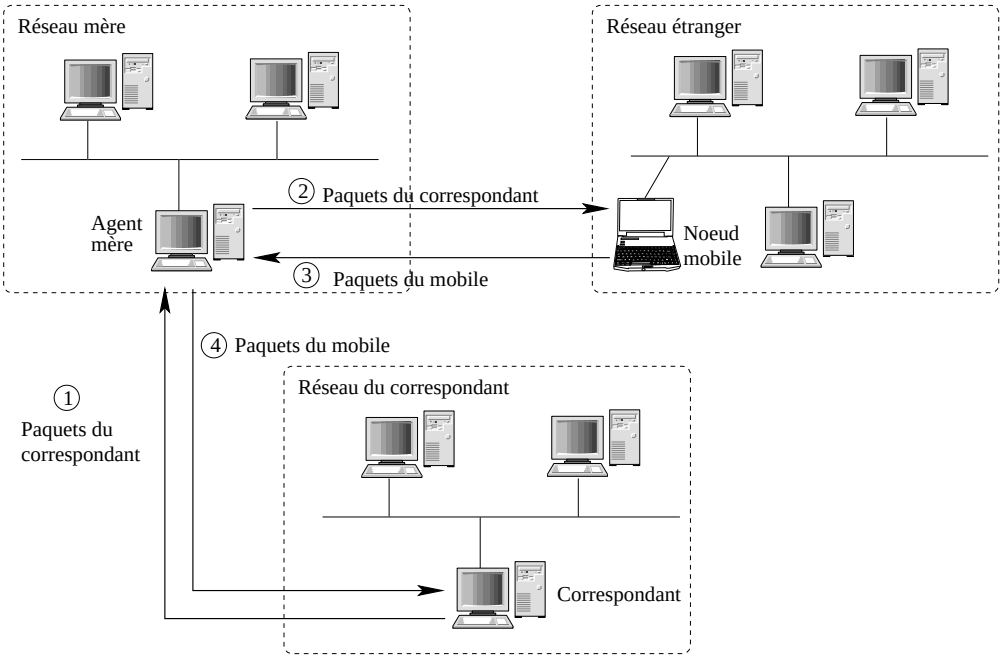

FIG. 2 – Le tunnel bidirectionnel.

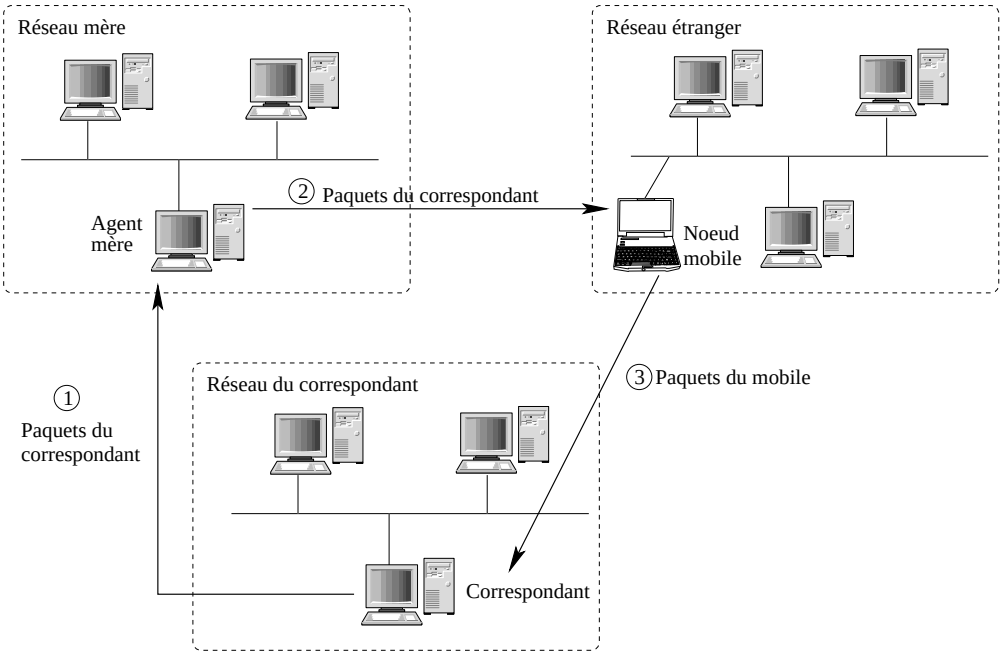

FIG. 3 – Le routage triangulaire.

Le routage triangulaire possède quelques problèmes de sécurité et est vulnérable à certaines attaques présentées dans la partie suivante, telles que les attaques par réflexion. Pour combler cette vulnérabilité il est nécessaire de vérifier la *Home Address option* soit par IPsec, soit par un *Binding Check*, c'est-à-dire vérifier qu'il existe une entrée valide pour cette association dans le *Binding Cache*.

Les deux modes de communications détaillés auparavant présentent l'inconvénient de générer beaucoup de trafic supplémentaire. C'est pourquoi un troisième mode de communication a été défini : le routage optimisé (*Route Optimization*).

3.3 Le routage optimisé

La figure 4 montre une optimisation du routage triangulaire, appelé routage optimisé. Le correspondant envoie son premier paquet à l'adresse mère du nœud mobile ①, ce message est intercepté par l'agent mère qui le fait suivre vers l'adresse temporaire courante du nœud mobile après consultation de son *Binding Cache* ②. Le nœud mobile recevant des messages de son correspondant par l'intermédiaire de son agent mère en déduit que son correspondant ne connaît pas son adresse temporaire courante. Le nœud mobile peut alors informer directement son correspondant de son adresse temporaire primaire en lui envoyant un message *Binding Update* ③. Le correspondant met à jour sa table d'association (*Binding Cache*) et peut acquitter le message en envoyant un *Binding Acknowledgement* ④. Le nœud mobile et son correspondant peuvent communiquer directement sans passer par l'agent mère du nœud mobile ⑤.

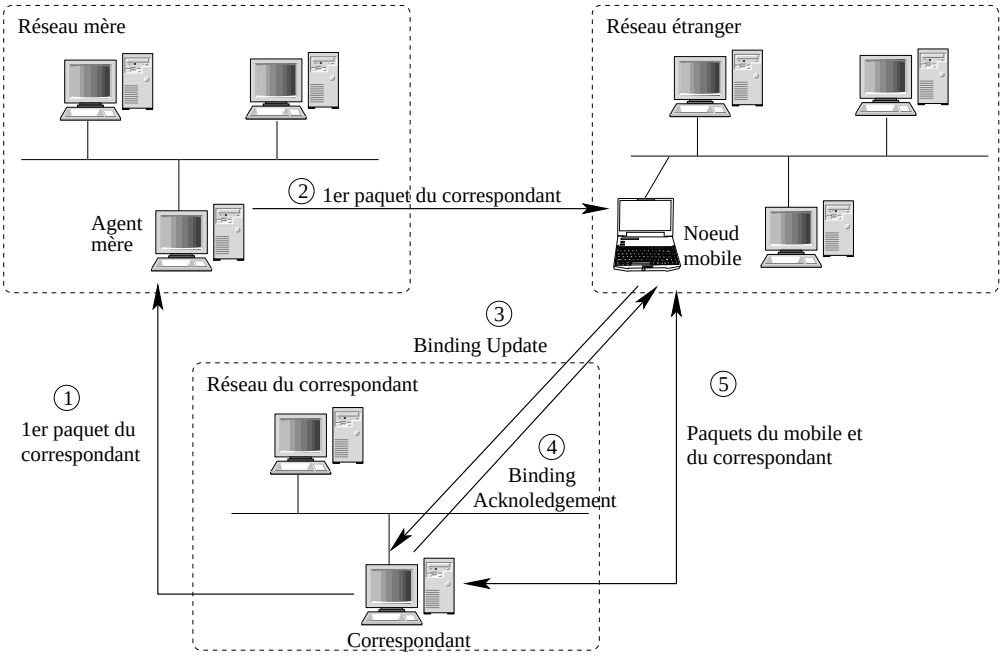

FIG. 4 – Le routage optimisé.

En théorie, le routage optimisé peut aussi être fait *a priori*. C'est-à-dire que si les deux entités communicantes connaissent leurs adresses respectives, elles peuvent s'envoyer des paquets sans passer par l'agent mère du nœud mobile.

4 Attaques contre MIPv6

En plus de toutes les attaques existantes contre IPv4 ou IPv6, la mobilité en introduit de nouvelles.

4.1 Attaques

Le protocole Mobile IPv6 repose sur des messages de signalisation envoyés par le nœud mobile afin d'avertir les entités désirant communiquer avec lui (agent mère ou correspondant) de l'utilisation d'une nouvelle adresse temporaire. La manipulation ou la création de ces messages de signalisation par un acteur

malveillant permet de mener des attaques contre le protocole de mobilité [NAA+04, Per96, Eur99]. Ces attaques peuvent avoir plusieurs buts différents :

- détourner le trafic en provenance ou à destination du nœud mobile
- créer un déni de service contre une cible donnée (n'importe quel nœud IPv6) ou innonder la cible de paquets
- remplir le cache d'association (*Binding Cache*) inutilement

4.1.1 Attaques visant à détourner le trafic

La figure 5 montre une attaque visant à détourner le trafic destiné à un nœud mobile.

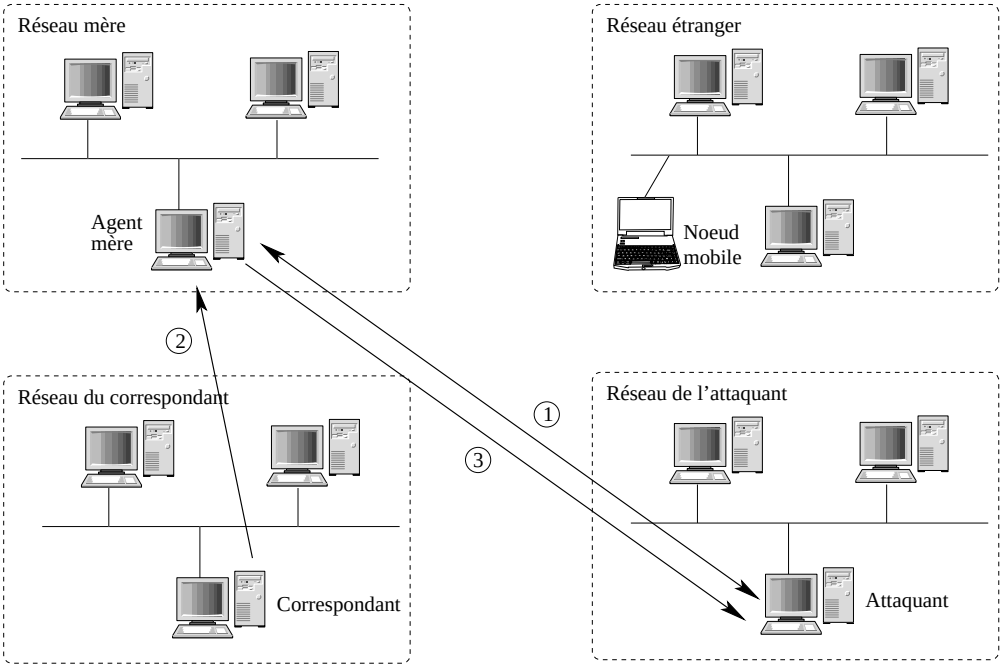

FIG. 5 – Attaque contre l'agent mère.

Si les messages de signalisation ne sont pas protégés, c'est-à-dire si leur source n'est pas authentifiée et si leur intégrité n'est pas garantie, un attaquant peut créer un faux message *Binding Update* informant que la nouvelle adresse du nœud mobile cible est l'adresse de la machine de l'attaquant. Puis l'attaquant envoie ce faux message à l'agent mère du nœud mobile cible ①. Si ce message n'est pas vérifié, l'agent mère mettra à jour sa table d'association et enverra tous les paquets qu'il reçoit à destination du nœud mobile ② vers la machine de l'attaquant ③.

L'attaquant peut aussi envoyer ce type de message directement au correspondant pour se faire passer pour le nœud mobile. Ce type d'attaque permet de détourner les communications à destination du nœud mobile cible.

4.1.2 Attaques visant à créer un déni de service ou à inonder une cible de paquets

La figure 6 présente un schéma d'attaque créant un deni de service. Un acteur malveillant envoie des messages *Binding Update* comprenant une fausse adresse source (*spoofing*) à un grand nombre de nœuds ①. Il indique dans ce message que sa cible possède une nouvelle adresse temporaire. Ainsi, tous les nœuds contactés enverront les paquets à destination de la cible vers cette nouvelle adresse ②. La cible est alors dans l'incapacité de recevoir des paquets provenant des nœuds contactés par l'attaquant et ainsi de leur fournir un service ou de recevoir les services de ces machines.

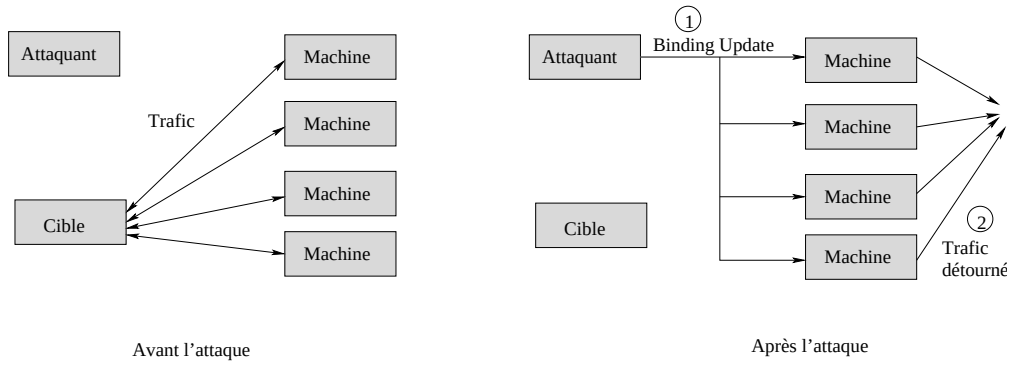

FIG. 6 – Attaque de déni de service.

Une attaque par innondation (*flooding*) possède un but similaire au déni de service, la figure 7 montre ce type d'attaque qui consiste à envoyer un très grand nombre de paquets vers la cible afin d'occuper toutes ses ressources. Celle-ci ne disposera alors plus des ressources nécessaires pour répondre aux paquets licites qu'elle pourrait recevoir. Un acteur malveillant peux dévier de gros trafics (flux video par exemple) vers une cible donnée en créant un faux message *Binding Update* comportant l'adresse de la cible ①. Le flux est ainsi dirigé vers la cible et l'attaquant n'a qu'à renvoyer des acquittement afin de garder le trafic en vie ②.

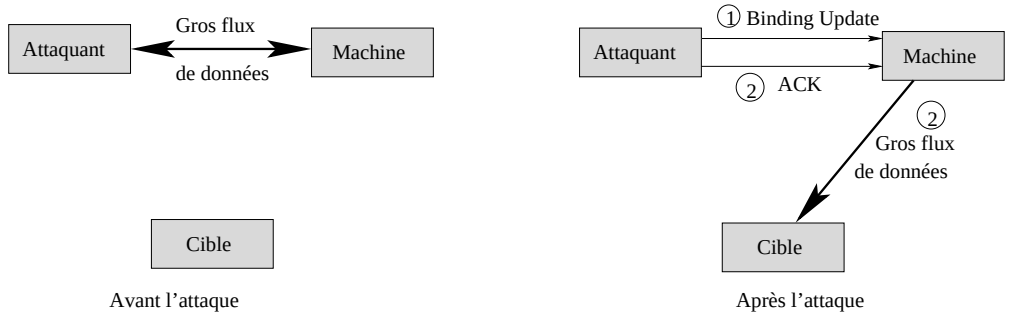

FIG. 7 – Attaque visant à innonder la cible.

4.1.3 Attaques visant à remplir le cache d'association *Binding Cache* inutilement

Cette attaque consiste à envoyer un grand nombre de messages *Binding Update* avec des adresses sources différentes au nœud mobile ou au correspondant. Cela a pour effet d'occuper les ressources de la cible et comme les adresses contenues dans les *Binding Update* sont des adresses IP utilisées sur l'Internet, la cible complète la mise à jour afin de créer une association dans sa table d'association (*Binding Cache*). Ainsi, l'attaquant remplit la table d'association de sa cible avec des associations inutiles ce qui empêche la cible de créer des associations dont elle aurait besoin et pourrait l'empêcher d'utiliser le routage optimisé à cause d'une pénurie de place dans sa table d'association.

4.2 Protection des messages de signalisation

Un mécanisme a été défini pour permettre au correspondant d'avoir une assurance raisonnable que le nœud mobile est bien celui qu'il prétend être. Il s'agit du mécanisme de *Return Routability* (figure 8).

Lorsque le nœud mobile utilise le mécanisme de *Return Routability* il envoie en même temps deux messages, un message *Care-of Test Init* directement au correspondant et un message *Home Test Init* à son agent mère qui le relaie vers le correspondant ①.

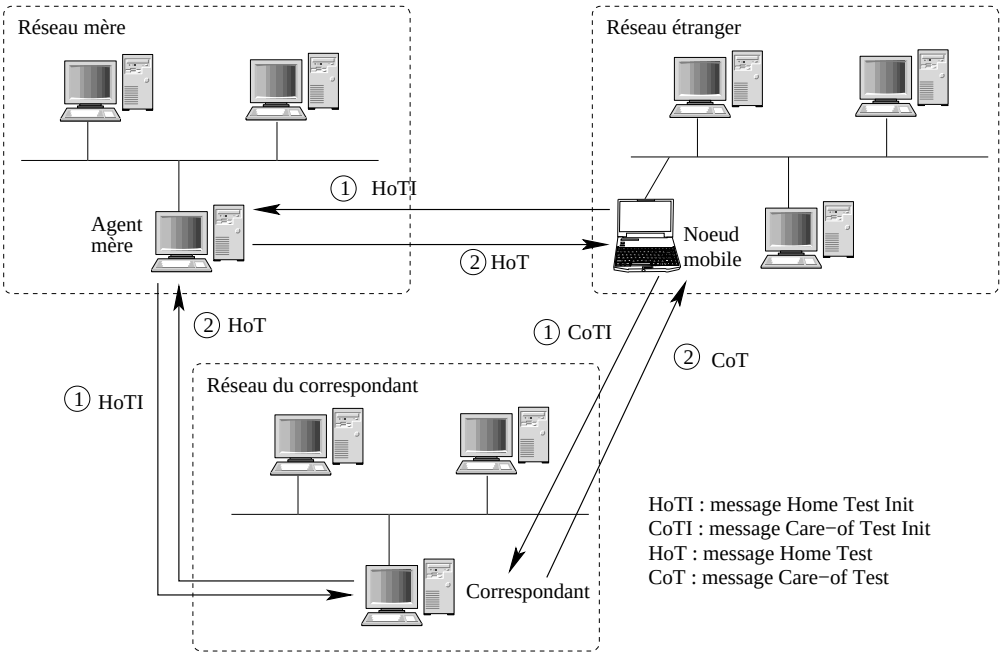

FIG. 8 – Le mécanisme de *Return Routability*.

Le correspondant reçoit ces deux messages et génère deux réponses qui dépendent du contenu des messages reçus. Le premier message (*Care-of Test*) est envoyé directement au nœud mobile et le second message (*Home Test*) est envoyé à l'adresse mère du nœud mobile. L'agent mère intercepte ce message et le fait suivre au nœud mobile. Le contenu de ces deux réponses permet de générer une clé qui est ensuite utilisé dans le message *Binding Update*.

Le problème est que ce mécanisme est faible au niveau de la sécurité car il s'appuie sur l'envoi coordonné de deux messages dont l'un passe par l'agent mère et il suppose qu'il n'y a pas d'acteurs hostiles près du correspondant et qu'ainsi il ne peut y avoir d'interception des paquets envoyés par le correspondant. Ceci ne peut être suffisant dans le cadre d'un emploi généralisé de ce protocole.

5 DNSSEC et MIPv6

5.1 Utilisation d'IPsec pour sécuriser la signalisation MIPv6

Un autre moyen existe pour sécuriser la signalisation MIPv6, il s'agit d'utiliser IPsec [KA98] en mode transport [ADD04]. IPsec fournit une authentification forte et serait donc une solution à la sécurisation des messages de signalisation MIPv6. Le problème de cette solution est de fournir une infrastructure globale pour que les certificats de tous les correspondants potentiels soient disponibles. L'utilisation d'une infrastructure DNSSEC [ALMR03, AAL$^+$03a, AAL$^+$03b, Gun03] résout le problème de disponibilité des certificats même dans le cas où le correspondant n'est pas rattaché à une PKI classique et permet d'authentifier les certificats récupérés. Les documents [ADD04] et [DC04] décrivent l'utilisation d'IPsec respectivement entre le nœud mobile et l'agent mère et entre le nœud mobile et le correspondant.

Le draft [Ric03] définit un nouvel enregistrement DNS (un Resource Record est la structure de données de base du DNS) dédié au stockage de clé IPsec. L'utilisation de cet enregistrement permet de conserver des clés IPsec associées à chaque machine dans le fichier de zone DNS. L'avantage est que le DNS est un service public et mondialement accessible. Ainsi chaque correspondant serait en mesure de récupérer la clé IPsec de la machine avec laquelle il veut communiquer. Cela peut se faire simultanément (sans véritable surcoût) lorsque le DNS est interrogé par l'appelant pour obtenir l'adresse IP de l'appelé. Les clés IPsec sont alors

utilisées pour sécuriser les messages de signalisation MIPv6. L'utilisation de l'enregistrement IPSECKEY permettrait de résoudre le problème de disponibilité des clés, de plus les mécanismes DNSSEC garantissent l'authentification et l'intégrité de la clé contenue dans cet enregistrement. Les entités de Mobile IPv6 ont alors à leur disposition les clés IPsec de tous leurs correspondants potentiels et peuvent ainsi utiliser IPsec pour sécuriser la signalisation MIPv6. IPsec fournit une bien meilleure sécurité des messages de signalisation que le mécanisme de *Return Routability* qui suppose qu'un attaquant ne se trouve pas sur le même réseau que le nœud mobile. Le draft [DC04] présente l'utilisation d'IPsec entre un nœud mobile et un correspondant utilisant le routage triangulaire ou le routage optimisé.

5.2 Modifier *racoon* pour qu'il vérifie par DNSSEC

Racoon est l'implémentation KAME/Linux2.6 du protocole IPsec IKE [HC98] de gestion des associations de sécurité. IKE consiste en un échange Diffie-Hellman avec une authentification mutuelle forte, assurée dans le mode qui nous intéresse par des signatures numériques.

Racoon implémente IKEv1, il ne supporte qu'un seul certificat de type X.509 qui peut être :

- échangé par une charge utile de type CERT (cas par défaut)
- spécifié directement dans la configuration sous la forme du nom de fichier contenant le certificat
- recherché par le DNS en fonction de l'identité de type ID_FQDN (le code incomplet prévoit la recherche via DNSSEC)

Dans le dernier cas, *racoon* fonctionne de la façon suivante : il prend la charge utile IDir (idendité du *responder*) qui doit être de type ID_FQDN (*Fully Qualified Domain Name*) et va rechercher via le DNS le CERT RR [Eas99] correspondant à ce FQDN. Le DNS n'étant pas sécurisé, on ne peut émettre aucune garantie quant à l'authenticité et à l'intégrité du certificat récupéré. L'idée est donc d'utiliser DNSSEC pour récupérer le CERT RR et de valider la signature associée afin de garantir l'intégrité et l'authentification de cet enregistrement.

5.3 Ajouter DNSSEC comme méthode de confiance à la fonction de vérification des certificats

Une autre utilisation de DNSSEC pour protéger la signalisation de Mobile IPv6 est d'ajouter DNSSEC comme méthode de confiance à la fonction *X509_verify_cert()* d'OpenSSL. Cette fonction vérifie un certificat en construisant une chaîne de confiance depuis le certificat donné en argument jusqu'à un certificat racine, c'est-à-dire un certificat auto-signé, en lequel on a confiance. Pour construire cette chaîne la fonction recherche le certificat de l'émetteur du certificat courant. Quand la chaine est construite, la fonction vérifie la confiance dans le certificat racine.

Le DNS (le CERT RR) peut être utilisé comme moyen de distribution de certificats, ou bien, quand les certificats présents dans les CERT RR sont toujours auto-signés (certificats racines ou clés encapsulées), comme moyen de validation des certificats, c'est-à-dire en s'assurant qu'une interrogation DNSSEC sur le nom de l'émetteur du certificat retourne bien ce certificat correctement signé.

En utilisant, dans la fonction *X509_verify_cert()*, ce type de validation par DNSSEC comme méthode de confiance on prolonge la validation X.509 en validation DNSSEC jusqu'au point d'entrée (*trust anchor* [KSL03]).

5.4 Utilisation du protocole SCVP

Le projet CADDISC/VERICERT [LM04] est un projet incitatif GET dont le but est d'améliorer la technologie des PKI classiques X.509, notamment en mettant en place une inter-connexion de PKI par DNSSEC et en déportant la validation des certificats par protocole SCVP (*Simple Certificate Validation Protocol*) [MHF04]. Pour cela, un prototype client/répondeur SCVP a été développé et une méthode *trust DNSSEC* a été ajouté à OpenSSL. Quand un validateur X.509 rencontre un certificat racine (certificat auto-signé en sommet de chaîne), au lieu d'utiliser une liste des certificats auxquels on fait confiance dans le système de fichiers, il va chercher par DNSSEC les CERT RR correspondants aux SubjectAltNames de type dNSName et compare les certificats valides (au sens de DNSSEC) obtenus au certificat racine : si les deux correspondent on peut leur faire confiance.

5.5 Le choix d'IDsA

Au vue de l'étude, il apparaît que le code actuel de *racoon* n'est pas sûr car il utilise le DNS au lieu du DNSSEC. Le projet IDsA a porté son choix sur l'amélioration de ce code et la mise en place d'une plate-forme utilisant ce *racoon modifié*. Ce sera l'objet du livrable 3.3.

Références

[AAL+03a] Arends (R.), Austein (R.), Larson (M.), Massey (D.) et Rose (S.). – Protocol Modifications for the DNS Security Extensions. – Draft IETF, work in progress, Dec 2003. draft-ietf-dnsext-dnssec-protocol.

[AAL+03b] Arends (R.), Austein (R.), Larson (M.), Massey (D.) et Rose (S.). – Resource Records for the DNS Security Extensions. – Draft IETF, work in progress, Dec 2003. draft-ietf-dnsext-dnssec-records.

[ADD04] Arkko (J.), Devarapalli (V.) et Dupont (F.). – Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. – RFC 3776, Jui 2004.

[ALMR03] Arends (R.), Larson (M.), Massey (D.) et Rose (S.). – DNS Security Introduction and Requirements. – Draft IETF, work in progress, Dec 2003. draft-ietf-dnsext-dnssec-intro.

[DC04] Dupont (F.) et Combes (J.M.). – Using IPsec between Mobile Nodes and Correspondent IPv6 nodes. – Draft IETF, work in progress, Avr 2004. draft-dupont-mipv6-cn-ipsec.

[Dro97] Droms (R.). – Dynamic Host Configuration Protocol. – RFC 2131, Mar 1997.

[Eas99] Eastlake (D.). – Storing Certificates in the Domain Name System. – RFC 2538, Mar 1999.

[Eur99] Eurescom, Projet P912, Security Guidelines for Mobility to IP. – Security Guidelines for the introduction of Mobility to IP, 1999.

[Gun03] Gundmundsson (O.). – Delegation Signer Resource Record. – RFC 3658, Dec 2003.

[HC98] Harkins (D.) et Carrel (D.). – The Internet Key Exchange (IKE). – RFC 2409, Nov 1998.

[HL01] Hunskaar (J.) et Lunde (T. A.). – *Mobility in IPv6.* – Master's Thesis, Agder College, 2001.

[JPA04] Johnson (D.), Perkins (C.) et Arkko (J.). – Mobility Support in IPv6. – RFC 3775, Jui 2004.

[KA98] Kent (S.) et Atkinson (R.). – Security Architecture for the Internet Protocol. – RFC 2401, Nov 1998.

[KSL03] Kolkman (O.), Schlyter (J.) et Lewis (E.). – DNSKEY RR Secure Entry Point Flag. – Draft IETF, work in progress, Dec 2003. draft-ietf-dnsext-keyrr-key-signing-flag.

[LM04] Laurent-Maknavicius (M.). – Les annuaires LDAP et DNSSEC au service d'une PKI globale. *In : 3ème rencontre francophone sur Sécurité et Architecture Réseaux (SAR'2004).* – Jui 2004.

[MHF04] Malpani (A.), Housley (R.) et Freeman (T.). – Simple Certificate Validation Protocol (SCVP). – Draft IETF, work in progress, Avr 2004. draft-ietf-pkix-scvp.

[NAA+04] Nikander (P.), Arkko (J.), Aura (T.), Montenegro (G.) et Nordmark (E.). – Mobile IP version 6 Route Optimization Security Design Background. – Draft IETF, work in progress, Avr 2004. draft-ietf-mipv6-ro-sec.

[Per96] Perkins (C.). – IP Mobility Support for IPv4. – RFC 3344, Oct 1996.

[Ric03] Richardson (M.). – A method for storing IPsec keying material in DNS. – Draft IETF, work in progress, Sep 2003. draft-ietf-ipseckeyrr.