Chiffrement Opportuniste et Mobilité IP

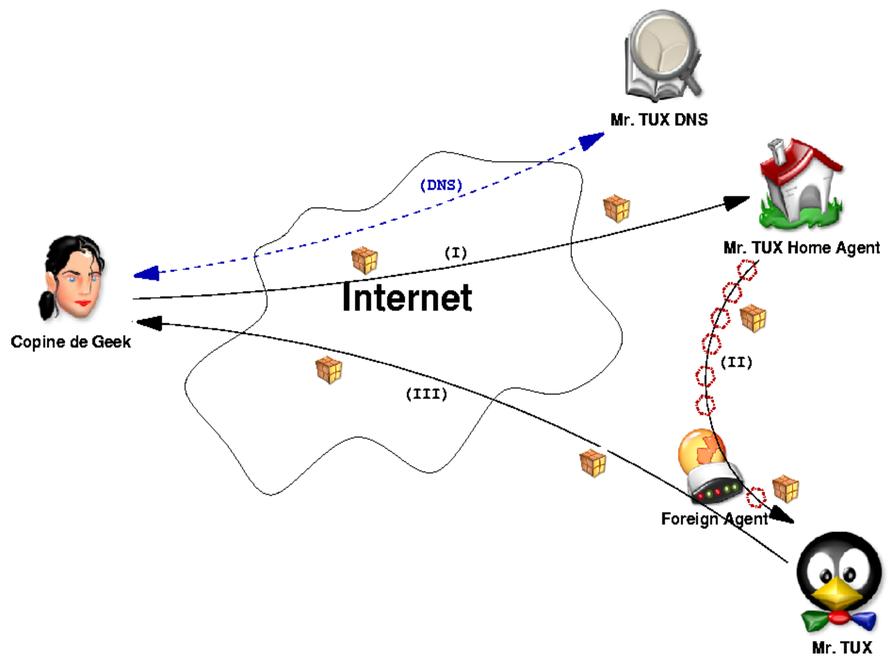
Une Étude de la mise en oeuvre d'une technique de Chiffrement Opportuniste dans un contexte de Mobilité IP.

Les Acteurs

Mr. TUX : Héros de nos aventures, cet utilisateur mobile à la mine placide est aussi qualifié par les médias de communiste, d'anarchiste, d'anti-gouvernementaliste, d'asocial, de socialiste, d'activiste intégriste. D'après nous, il s'agit surtout d'un palmipède grand amateur de poissons. www.kernel.org .

Le DNS est le service de noms d'Internet. A la manière d'un annuaire, il permet d'obtenir une adresse à partir d'un nom et vice-versa. Par exemple, par le truchement du DNS, www.coca-cola.com devient 212.73.194.142. On peut aussi stocker des clefs publiques et des informations de délégation dans le DNS.

Copine de Geek est une biologiste spécialisée dans l'étude des gnous et des manchots. Plus d'explications sur son site : www.copinedegeek.com .



A - DNS, Mobilité

Domain Name System (DNS)

C'est le service des renseignements (le ``12'') : il convertit les noms en adresses et vice-versa. Il peut aussi héberger des clefs publiques.

C'est une base de données répartie ; ses échanges sont ici simplifiés.

Routage Triangulaire

En Mobilité IP, **Mr. TUX** est toujours joignable par son adresse principale ;Si on considère le scénario ci-contre :

[1] Après avoir obtenu l'adresse de **Mr. TUX** par le **DNS**, **Copine de Geek** ``emballe'' des informations dans des paquets adressés à **Mr. TUX**.

[2] Les paquets sont transférés au bureau de poste (**Home Agent**), lequel opère un ``transfert de courrier'' vers le **Foreign Agent**. **Mr. TUX** reçoit finalement les paquets.

[3] **Mr. TUX** renvoie des réponses à **Copine de Geek**.

Ce cheminement s'appelle le **routage triangulaire**. Il permet de joindre **Mr. TUX** lors de ses déplacements. Par la suite,

- Le routage triangulaire n'est pas représenté ; il s'applique implicitement.
- L'acheminement entre le **Home Agent** et **Mr. TUX** est sécurisé (ils se connaissent et protègent leurs communications).

B - Le Mobile Indépendant

Dans ce profil, **Mr. TUX** prend en charge ses besoins de sécurité.

Détails des échanges

[1] **Mr. TUX** interroge le **DNS** et obtient la **Passerelle de Sécurité** de **Mr. RMS** et la clef publique de cette dernière.

[2] **Mr. TUX** initie des échanges avec la **Passerelle** pour créer un **lien sécurisé**.

[3] La **Passerelle** ignore qui est **Mr. TUX** et interroge donc le **DNS** pour obtenir sa clef publique.

[4] La négociation s'achève avec création du **lien sécurisé**.

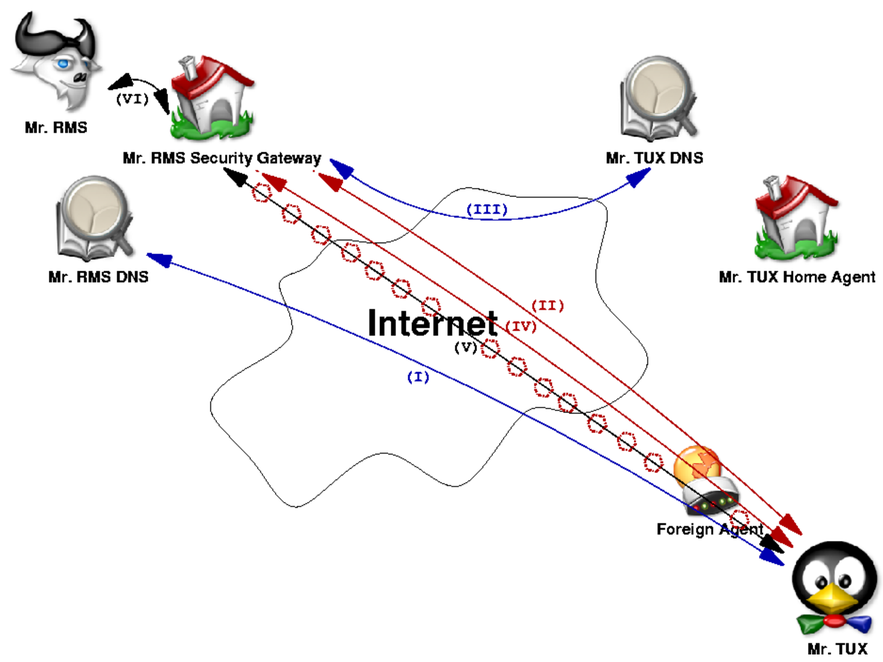
[5] **Mr. TUX** envoie ses paquets par le **lien sécurisé**.

[6] La **Passerelle** déchiffre l'information et l'achemine à **Mr. RMS**.

Remarques

La négociation permettant d'établir un **lien sécurisé** construit des clefs cryptographiques grâce à un **échange de Diffie-Hellman authentifié**.

Les clefs publiques, récupérées dans le **DNS**, permettent de vérifier l'authenticité des informations envoyées et de procéder à cet échange en toute sécurité.



Les Acteurs (Suite)

Lien sécurisé par IPsec (assure l'authenticité, l'intégrité, et la confidentialité des données).

Les paquets sont les convoyeurs d'Internet; ils emballent les informations, un peu à la manière des colis postaux.

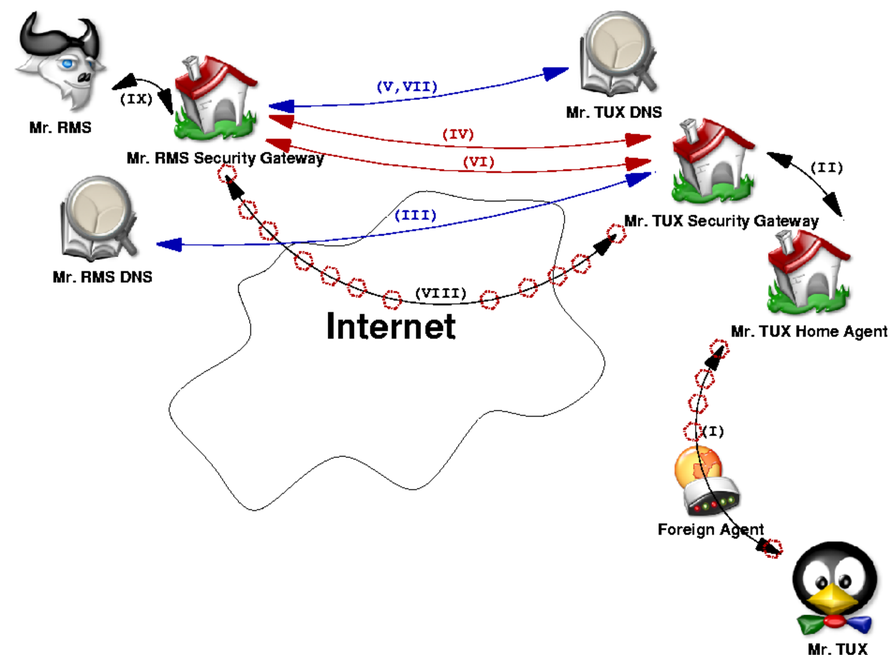
Ce symbole permet de représenter indifféremment une passerelle de sécurité ou un home-agent. D'un point de vue général, il s'agit d'un routeur et son rôle est de décider de l'acheminement des paquets en fonction de certains critères, par exemple en fonction de la disponibilité d'un mobile ou des contraintes de sécurité.

Les Acteurs (Fin)

Le Foreign Agent est un équipement auquel Mr. TUX se connecte quand il est mobile. Le Foreign Agent lui donne alors accès à Internet.

Mr. RMS est gnou sédentaire ; il délègue tous ses besoins de sécurité à un système placé à l'entrée de sa maison (**Passerelle de Sécurité**). Il pense que les droits civils doivent être protégés, notamment la vie privée. Par conséquent, à chaque fois qu'il peut utiliser de la cryptographie, il le fait.

Jean-Jacques Puig est Doctorant. Il s'est servi de vim (www.vim.org), de fop (xml.apache.org/fop), de xfig (www.xfig.org) et de gimp (www.gimp.org) pour créer ce poster.



C - Le Mobile Couvé

Dans ce profil, **Mr. TUX** délègue les traitements de sécurité à sa **Passerelle de Sécurité**.

Détails des échanges

[1] **Mr. TUX** envoie désormais ses paquets vers son **Home Agent** (mécanisme de **Reverse Tunneling**).

[2] Le **Home Agent** transmet les paquets à la **Passerelle de Sécurité**, qui les place en attente.

[3] La **Passerelle de Sécurité** recherche la **Passerelle de Sécurité** de **Mr. RMS** dans le **DNS**, et récupère sa clef publique.

[4] La **Passerelle de Sécurité** entame les négociations en vue d'établir le **lien sécurisé**.

[5] La **Passerelle de Sécurité de Mr. RMS** consulte le **DNS** pour obtenir la clef publique de la **Passerelle de Sécurité de Mr. TUX**.

[6] La négociation s'achève, le **Passerelle de Sécurité de Mr. TUX** annonce qu'elle transmet des données de Mr. TUX.

[7] La **Passerelle de Sécurité de Mr. RMS** vérifie dans le DNS que son interlocuteur a toute légitimité pour acheminer les paquets de **Mr. TUX** (vérification de la **délégation**).

[8] La **Passerelle de Sécurité de Mr. TUX** envoie les paquets placés en attente à travers le lien sécurisé.

[9] La **Passerelle de Sécurité de Mr. RMS** déchiffre les paquets et les transfère à **Mr. RMS**.

D - Remarques

Le Mobile Prudent

A mi-chemin entre les deux modèles précédents, nous avons établi le comportement d'un mobile qui décide de façon dynamique s'il se comporte en Mobile Indépendant ou en Mobile Couvé.

Ce ``Mobile Prudent'' joue pour cela sur une incohérence volontaire des données indiquées par le **DNS** suivant si on demande des informations à partir de son nom ou à partir de son adresse.

Les Protocoles

Les protocoles utilisés dans les scénarios précédents sont issus de la suite IPsec.

La construction des clefs et des associations de sécurité est effectuée par **IKE (Internet Key Exchange)**.

La protection des paquets est assurée par **AH (Authentication Header)** et/ou **ESP (Encryption Security Payload)** en mode tunnel.

E - Perspectives

Publication

Ce travail a fait l'objet d'une soumission à CFIP (Conférence Francophone sur l'Ingénierie des Protocoles) 2003 (en attente de réponse à ce jour).

Développements

De nouvelles techniques de Chiffrement Opportuniste apparaissent. Il sera intéressant d'analyser leurs interactions et leurs spécificités.

Le **Routage Optimisé**, encore à l'étude, ouvre des perspectives d'assouplissement des techniques présentées (gain de performances significatif).

Lors d'un **Hand-Over** de **Mr. TUX**, le **lien sécurisé** est rompu. Des opportunités de résolution de ce problème s'ouvrent avec le **transfert de contexte pour les associations de sécurité**.

Sécurité des Réseaux IP

Jean-Jacques Puig , Doctorant.

Maryline Laurent-Maknavicius , Professeur.

Samovar CNRS UMR 5157 ,
Pièce A109,
9, Rue Charles Fourier,
91011 Évry,

Ce document a été élaboré à l'occasion des Journées des Doctorants UEVE.

Les icônes utilisées dans ce poster font parties d'un projet de FreshMeat (www.freshmeat.net).