Jean-Jacques PUIG
Département Logiciels-Réseaux (LoR),
Institut National des Télécoms (INT)
Tél: 01.60.76.44.65 Fax: 01.60.76.47.11
Mail: jean-jacques.puig@int-evry.fr

SÉCURITÉ IP

I Présentation de IP

IP est un protocole de télécommunication défini par un organisme international, l'IETF. Les objectifs historiques d'IP, définis par le Département de la Défense Américain, sont l'interconnexion de réseaux hétérogènes et la possibilité d'acheminer des paquets d'information, appelés "paquets IP", par des routes multiples. Ainsi, même si une attaque nucléaire détruisait une partie du réseau, l'information serait toujours en mesure de se frayer un chemin jusqu'à son destinataire.

Cependant, IP est aux télécommunications ce que la carte postale est au courrier: le paquet IP peut être perdu, intercepté, lu, détruit, modifié ou avoir été envoyé sous l'identité d'un autre expéditeur. De plus, le paquet peut être dupliqué et arriver chez le destinataire en plusieurs exemplaires.

II La sécurité d'Internet

L'IETF a défini une couche de sécurité pour IP. Cette dernière, nommée "IPsec", est principalement constituée de trois catégories interdépendantes de protocoles et de processus:

- Communication sécurisée: authentification, intégrité, confidentialité des paquets IP, protection des communications contre les attaques par duplication des paquets ("replay attacks").
- Sécurité de contextes spécifiques: utilisateurs mobiles, dissimulés dans des sous-réseaux privés, communication de groupe, etc.
- Négotiation de paramètres de sécurité: clefs, périodes de rafraîchissement, services cryptographiques, algorithmes, politiques de sécurité et d'audit.

IP n'a pas été conçu dans l'optique de supporter des fonctionnalités cryptographiques, aussi de nombreux points restent à définir ou à redéfinir, comme par exemple les protocoles de constitution de clefs ou le support de l'anonymat. Par ailleurs, ces services peuvent menacer le fonctionnement habituel du réseau. Ainsi, un "firewall" ne peut pas analyser un paquet chiffré par IPsec s'il ne dispose pas des clefs nécessaires. Certains problèmes pourront être résolus; d'autres, inhérents aux limitations théoriques du protocole, seront insurmontables.

III Orientation de la Thèse

Cette thèse, entamée en octobre 2001, consiste dans un premier temps à faire une analyse critique d'IPsec, de son impact sur un réseau opérationnel, de son niveau de sécurité réel. Il ressortira de cette étude tout un ensemble de situations dans lesquelles l'utilisation d'IPsec est impossible ou dangereuse.

Des solutions de sécurité devront alors être apportées dans ces contextes. Ces solutions seront bien sûr des protocoles ou des processus cryptographiques, et feront l'objet de publications auprès de l'IETF.