Chapitre 5 : IPSec

SÉcurité et Cryptographie

2013-2014

Sup Galilée INFO3

Sécurité des réseaux ?

Confidentialité : Seuls l'émetteur et le récepteur légitime doivent être en mesure de comprendre le contenu du message. L'émetteur chiffre le message, et le récepteur le déchiffre.

Authentification : L'émetteur et le récepteur doivent être certains de l'identité de leur correspondant.

Intégrité et non répudiation : L'émetteur et le récepteur doivent être certains que le message n'a pas été altéré pendant sa transmission. L'émetteur ne doit pas pouvoir nier l'avoir envoyé ni le récepteur l'avoir reçu.

Disponibilité : Les services doivent être accessibles.

Quelques exemples d'attaques

Écoute : Interception de messages.

Insertion active de message dans la connexion (on forge des faux messages).

Imitation : Falsification de l'adresse source dans le paquet.

Man-in-the-middle : Prise de contrôle de la communication en cours en se faisant passer pour l'émetteur ou le récepteur.

"Denial of service attack" : Empêcher qu'un service soit utilisable (par exemple par saturation de ses capacités).

Rejeu.

La sécurité réseau

Il existe plusieurs façons d'appliquer la sécurité sur un réseau.

- Au niveau applicatif : PGP, SSH (secure shell), HTTPS, FTPS.

- Au niveau session: SSL (Secure Sockets Layer).

- Au niveau réseau : IPSec.

(Couches du modèle OSI : 1. Physique (câbles), 2. Liaison (adresse MAC), 3 Résau (adresse IP), 4. Transport (connexion bout à bout), 5. Session, 6. Présentation, 7. Application.)

IP Security

- IPSec est intégré dans IPv6.

- Pourquoi IPv6 ?

    1. Grande capacité d'adressage (128 bits plutôt que 32 bits en IPv4).
    2. Routage simplifié.
    3. Sécurisation native des communications (IPSec).
    4. Protocole et architecture gérant la mobilité (même adresse pour une machine connectée à des réseaux différents).

Standardisation

- Standard développé à l'IETF (Internet Engineering Task Force).

- Premier RFC (Request For Comments) en 1995 sans la gestion des clefs.

- Second RFC en 1998 avec la gestion des clefs IKE (Internet Key Exchange).

- Commun à IPv6 et IPv4 (à cause de la lenteur du déploiement d'IPv6).

Apports d'IPSec

- Couche réseau pour le chiffrement et l'authentification.

- Solution flexible pour déployer des politiques de sécurité à grande échelle.

- Services fournis : confidentialité, intégrité, authentification de la source, contrôle d'accès, non rejeu.

Protocoles formant IPSec

- AH (Authentification Header).

- ESP (EncapSuled Payload).

- IKE (Internet Key Exchange, RFC 4306) : Avant qu'une transmission IPSec puisse être possible, IKE est employé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clefs partagées.

- ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408).

- OAKLEY (RFC 2412) : protocole d'échange de clef générique.

Encapsulation

Le paquet IP prend la forme suivante : En-tête IP, En-tête IPSEC (AH/ESP), Données IP (chiffrées).

Chaque paquet IP est chiffré et/ou authentifié.

Il existe deux modes :

1. Transport : en-tête non modifíe.
2. Tunnel : encapsulation dans un nouveau paquet IP.

Mode transport

- Pour la confidentialité : seules les données sont chiffrées (la partie payload du paquet IP). Le mode transport est utilisé pour les communications dites hôte à hôte (Host-to-Host).

- Implémenté au-dessus de la couche IP.

Mode Tunnel

- Idéal pour la mise en place de VPN (Virtual Private Network).

- Dans ce mode le paquet IP prend la forme suivante : Nouvelle en-tête IP, En-tête IPSec, Ancienne en-tête IP, données. Du coup on peut chiffré complétement tout l'ancien paquet IP. En mode tunnel, c'est donc la totalité du paquet IP qui est chiffré et/ou authentifié. Le paquet est ensuite encapsulé dans un nouveau paquet IP avec une nouvelle en-tête IP. Le mode tunnel est utilisé pour créer des réseaux privés virtuels permettant la communication de réseau à réseau (ex. entre deux sites distants), d'hôte à réseau (ex. accès à distance d'un utilisateur) ou bien d'hôte à hôte (ex. messagerie privée.)