Sécurité des réseaux
IPSec

A. Guermouche

Plan

Plan

Pourquoi?

- Premier constat sur l'aspect critique de la sécurité dans internet en 1994 (RFC 1636).
- Multiplications des attaques de type spoofing (usurpation d'indentité) et d'écoute clandestine du contenu du trafic.
- Nécessité de concevoir des mécanismes d'autentificatione et de chiffrement pour IP.

Applications et Propriétés

Quelques applications :

Sécuriser une connexion de sucursale sur Internet. Établir un réseau privé virtuel sécurisé.

Accès distant sécurisé sur internet. Accès sécurisé à un réseau distant (pour bénificier des services offerts par ce réseau).

Autenticité des paquets reçus. IPSec peut être utilisé pour assurer l'autentification lors des communications entre les machines concernées.

Avantages :

- Possibilité d'utilisation uniquement sur des communications spécifiques (sans perturber les autres communications).
- IPSec est au-dessous de la couche de transport (TCP, UDP); il est donc transparent aux applications (possibilité d'accroître la sécurité sans modifier les applications de plus haut niveau).
- Une fois mis en place, IPSec est transparent aux utilisateurs.

IPSec (1/2)

IPSec est décrit dans les RFC 2401, 2402, 2406 et 2408. IPSec fournit :

- Un protocole de d'authentification indiqué par l'en-tête d'authentification (`AH` (*Authentication Header*).
  - Contrôle d'accès.
  - Authentification de l'origine des données.
  - Rejet de paquets rejoués.
- Un protocole combiné chiffrement authtification (`ESP` (*Encapsulating Security Payload*)).
  - Confidentialités (chiffrement).
  - Confidentialités limitée au flot du trafic.

IPSec (2/2)

	AH	ESP (chiffrement)	ESP (chiffrement + authentification)
Contrôle d'accès	x	x	x
Intégrité hors connexion	x		x
Authentication de l'origine des données	x		x
Rejet des paquets rejoués	x	x	x
Confidentialité		x	x
Confidentialité du flot du traffic		x	x

Table: Services d'IPSec.

Paramètres d'associations de sécurité

- Une association de sécurité (AS) est une relation en sens unique entre un emetteur et un destinataire qui garantit les services de sécurité pour le trafic généré.
- Des services de sécurité sont alloués à une AS pour utiliser AH ou ESP mais pas les deux.
- Une AS est définie par trois paramètres :
  Index de paramètre de sécurité (IPS). Une chaîne binaire assignée à cette AS et ayant une signification locale.
  Adresse IP de destination.
  Identification du protocole de sécurité. Il indique si l'association est AH ou ESP.
- Plusieurs AS peuvent être combinées.
- Les associations entre AS et type de trafic se font par le biais d'une base de donnée de politique de sécurité (SPD (*Security Policy Database*)).

Mode d'utilisation (1/3)

Mode transport.

- Assure la proptection pour les protocoles de la couche transport (information utile d'un paquet IP)
- ESP chiffre (et optionnellement authentifie) uniquement l'information utile du paquet IP (l'en-tête reste inchangé).
- AH authentifie l'information utile IP et des parties de l'en-tête IP.

Mode tunnel.

- Assure la protection du paquet IP tout entier.
- Après l'ajout des champs AH ou ESP le paquet entier est traité comme l'information utile du paquet IP externe.
- Une (ou les deux) extrémité de l'AS doit être une passerelle de sécurité (firewall, passerelle implémentant IPSec, . . .).

Mode d'utilisation (2/3)

	Mode Transport	Mode Tunnel
AH	Authentifie l'information utile IP + certains champs de l'en-tête IP	Authentifie le paquet IP entier + certains champs de l'en-tête externe
ESP	Chiffre l'information utilse IP	Chiffre tout le paquet IP
ESP (avec authentification)	Chiffre l'information utile IP et authentifie l'information utile IP	Chiffre et authentifie le paquet tout entier

Table: Fonctionnalité des modes tunnel et transport.

Mode d'utilisation (3/3)

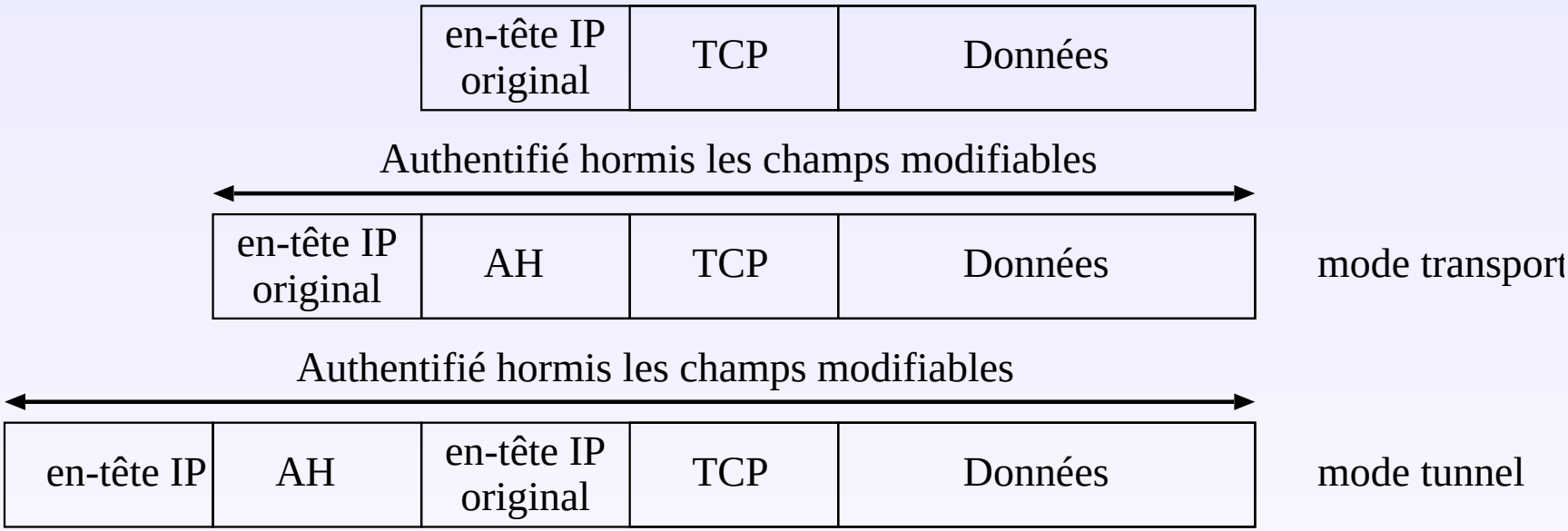

Figure: Portée de l'authentification AH.

Mode d'utilisation (3/3)

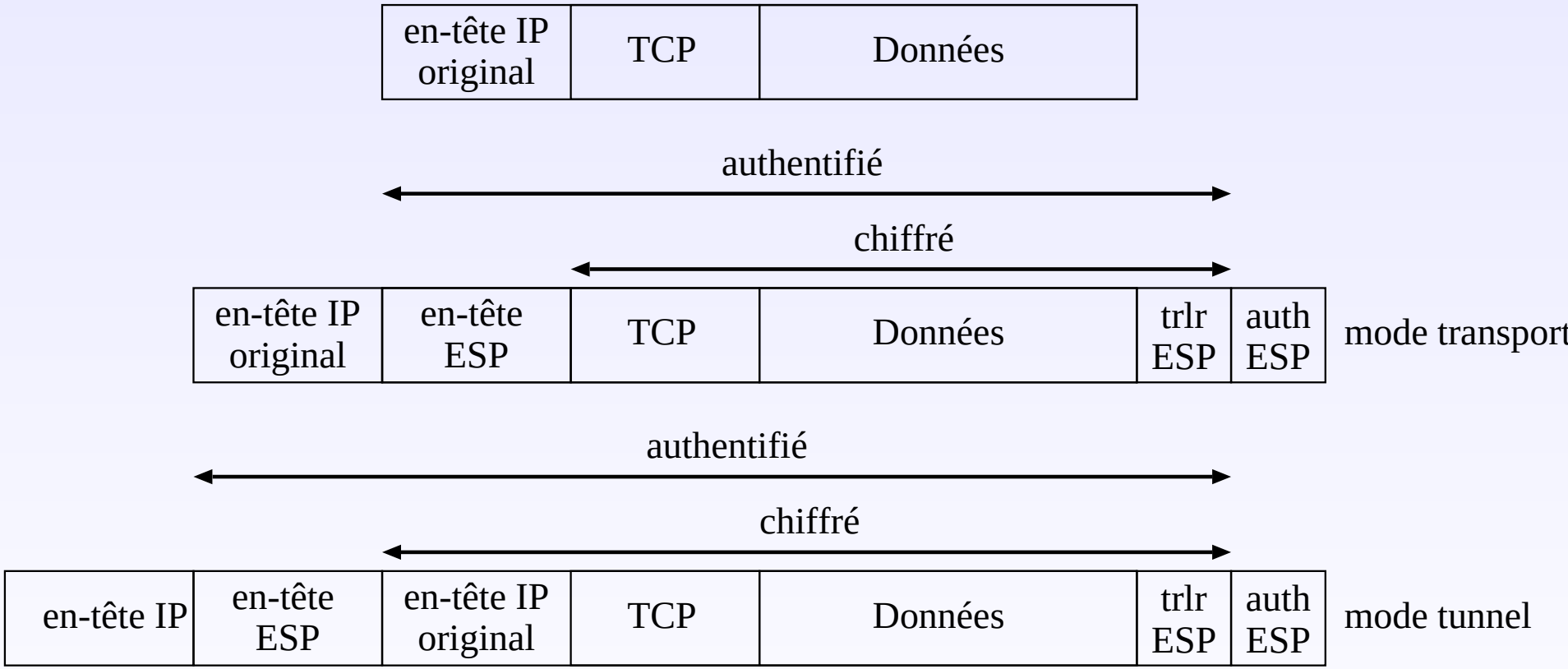

Figure: Portée de l'authentification et du chiffrement ESP.

AH

- L'en-tête d'authentification assure :
  - l'intégrité des données
  - l'authentification des paquets IP.
- L'authentification est basée sur l'utilisation d'un code d'authentification de message (MAC, *Message Authentication Code*).
- AH permet entre autre de détecter le rejeu.
- AH doit supporter HMAC-MD5-96 et HMAC-SHA-1-96.

Authentification de messages

Plusieurs algorithmes d'authentification de messages existent :

- Authentification à l'aide d'une clé secréte (MAC).
  - Authentification du message basée sur une clé secréte partagée par l'emetteur et le récepteur.
  - Mécanisme coûteux pour des messages de petite taille.
- Fonctions de hachage.
  - Construire un résumé du message et l'envoyer.
- Fonctions de hachage sécurisées (SHA-1, MD5, . . .).
  - Fonctions vérifiant des propriétés de robustesse (telles que l'"impossibilité" de deviner le contenu d'un message à partir de son résumé).

Solution retenue est l'authentification à l'aide de HMAC :

- Combiner MAC et des fonctions de hachage sécuriées (SHA-1).
- Avantages : Rapidité du mécanisme d'authentification, plusieurs algorithmes de hachages cryptographiques sont disponibles.

Service anti-rejeu

Attaque par rejeu. Un attaquant obtient une copie d'un message valide et la transmet ultérieurement à la destination.

Fonctionnement:

- Lorsqu'une nouvelle AS est établie, l'emetteur initialise un numéro d'ordre à zéro.
- Chaque fois qu'un paquet est envoyé à cette AS, l'expéditeur incrémente la valeur et la place dans le champ numéro d'ordre de l'en-tête AH.
- Le destinataire ne doit pas permettre au numéro d'ordre d'effectuer un cycle de 2^{32}-1 à 0 (pour éviter d'avoir plus d'un paquet valide avec le même numéro d'ordre).

Service anti-rejeu

Attaque par rejeu. Un attaquant obtient une copie d'un message valide et la transmet ultérieurement à la destination.

Fonctionnement:

- Au niveau du récepteur :
  - Créer une fenêtre de réception des paquets IP (Les paquets peuvent arriver dans le désordre) de taille W.
  - Le numéro d'ordre le plus élevé jusqu'ici (N) est noté à l'extrémité droite de la fenêtre.
  - Pour n'importe quel paquet correctement reçu ayant un numéro d'ordre compris entre N-W+1 et N, la position correspondante est marquée.

Service anti-rejeu

Attaque par rejeu. Un attaquant obtient une copie d'un message valide et la transmet ultérieurement à la destination.

Fonctionnement:

- Au niveau du récepteur :
  - À la réception d'un nouveau paquet :
    1. Si le paquet est nouveau et si le code MAC est valide, la position correspondante est marquée.
    2. Si le paquet reçu est à droite de la fenêtre et s'il est correctement authentifié, la fenêtre est avancée de sorte que le numéro d'ordre devienne la nouvelle valeur de N.
    3. Si le paquet n'est pas correctement authentifié ou s'il a un numéro d'ordre à gauche de la fenêtre, il est détruit.

ESP

ESP fournit :

- des services de confidentialités.
- un mecanisme anti-rejeu.
- un mécanisme d'authentification.

ESP supporte différents algorithmes de cryptage :

- 3DES
- RC5
- IDEA
- CAST
- Blowfish
- ...

Gestion des clé

- La gestion des clés implique la détermination de la distribution des clés secrètes.
- Une transmission classique nécessite 4 clés : deux paires de transmissions et de réceptions pour AH et ESP.
- IPSec supporte deux types de gestions :

  Manuelle. Un administrateur configure manuellement chaque système avec ses propres clés.

  Automatique. Un système automatisé permet une création à la demande de clés pour les AS.
- Le protocole de gestion de clés automatisé pour IPSec est ISAKMP/Oakley.

  Protocole d'Oakley. Un protocole de détermination de clés basé sur l'algorithme de Diffie-Helman avec une sécurité ajoutée.

  ISAKMP. Un protocole fournissant un cadre pour la gestion des clés, et des formats pour la négociations des attributs de sécurité.

Protocole de Diffie-Hellman

- 2 paramètres doivent être connus par les deux paires : q (un grand nombre premier) et a une racine primaire de q.

rappel :

a est racine primaire de $q \Leftrightarrow$ chaque autre entier, modulo q, est juste une puissance de a.

- Les paires A et B tirent aléatoirement deux nombres X_A et X_B respectivement (ils correspondent aux clés privées de A et de B).
- A transmet $Y_A = a^{X_A} mod q$ et B fait de même avec Y_B. (Y_A et Y_B sont les clés publiques de A et B)
- La clé de session est alors calculée :

$$K = (Y_B)^{X_A} mod q = (Y_A)^{X_B} mod q = a^{X_A X_B} mod q$$

Faiblesses de Diffie-Hellman

- Pas d'authentification entre les deux extrémités de la communication : MIM.
- Coût des calculs à réception du premier message : DOS.

Oakley:

- Utilisation de cookies pour éviter les attaques par déni de service.
- Les deux parties négocient un groupe (consiste à spécifier les paramètre globaux de Diffie-Hellman).
- Authentification des échanges du protocole de Diffie Hellman.
- Utilisation de nonces pour prévenir les attaques par rejeu.

Protocole d'Oakley

Exemple :

- (E) envoie un message en y incluant un cookie, le groupe à utiliser pour DH, et sa clé publique DH. De plus, il ajoute les algorithmes d'encryption, fonction de hachage et algorithmes d'authentification à disponible. Enfin, il y ajoute son identifiant et celui de (R) ainsi qu'un nonce ainsi qu'une signature générée à l'aide de clé privée DH de (E).
- (R) vérifie d'abord la signature. Il acquite le message en envoyant à (E) le contenu du message initial plus tout ce qui le concerne (l'algorithme sélectionné, le nonce, le cookie, ...).
- (E) vérifie la signature puis acquite le tout. Le nonce permet de détecter le rejeu.

ISAKMP : est le plus plus populaire des IKE (IPSec Key Exchange)

- Protocole pour la négociation des associations de sécurité.
- Utilise le protocole d'Oakley
- Nécessite deux phases : Une première pour créer un canal sécurisé pour le dialogue de la phase 2 où les vrais paramètres de sécurité sont négociés.

IPSec en pratique

Plusieurs implémentations sont disponibles :

- NETKEY
- KLIPS