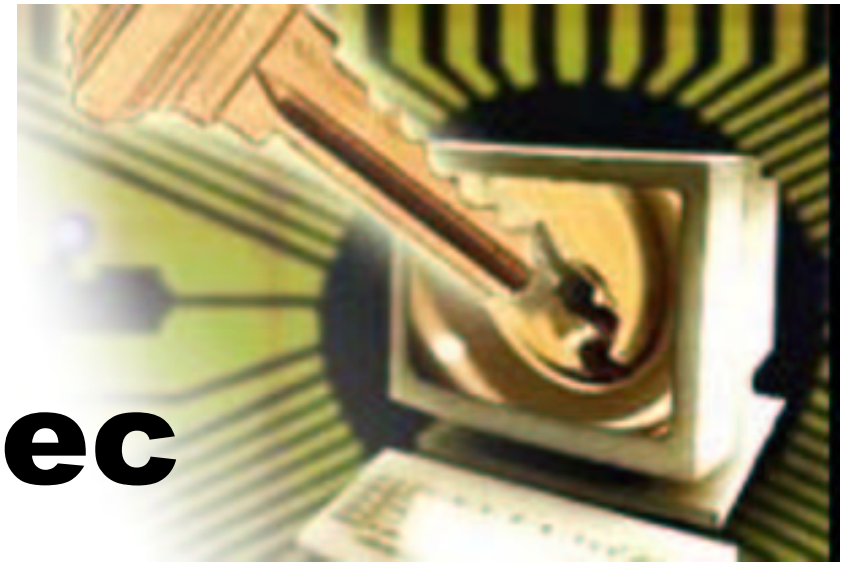


IPsec

Sécurité dans la couche *Réseau*

Daniel Wasserrab <dwasserr@ens-lyon.fr>
Andreas Wundsam <awundsam@ens-lyon.fr>

Articulation

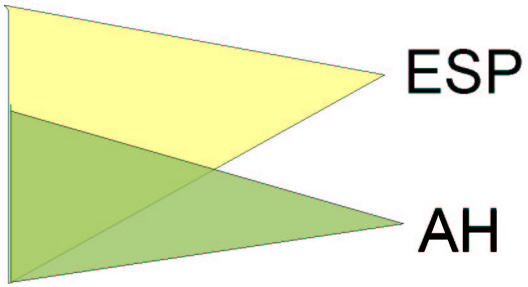
- 1. Introduction
  - a) Définition
  - b) IPsec vs. protocoles de la couche application
  - c) Application primaire: VPN
- 2. Les protocoles
  - a) IKE
  - b) AH
  - c) ESP
- 3. Modes d'opérations: transport versus tunnel
- 4. Limitations et problèmes

1.a) Définition

- IPsec: Système de protocoles fournissant de la sécurité pour la pile de protocoles IP
- basé lui-même sur IP (routage standard dans l'Internet)
- Conçu pour IPv6, mais adapté comme option pour IPv4
- standard ouvert, definit par l'IETF (RFC 2401)
  => en théorie, tous les machines implementantes le standard peuvent communiquer en sécurité

1.a) La sécurité, c'est...

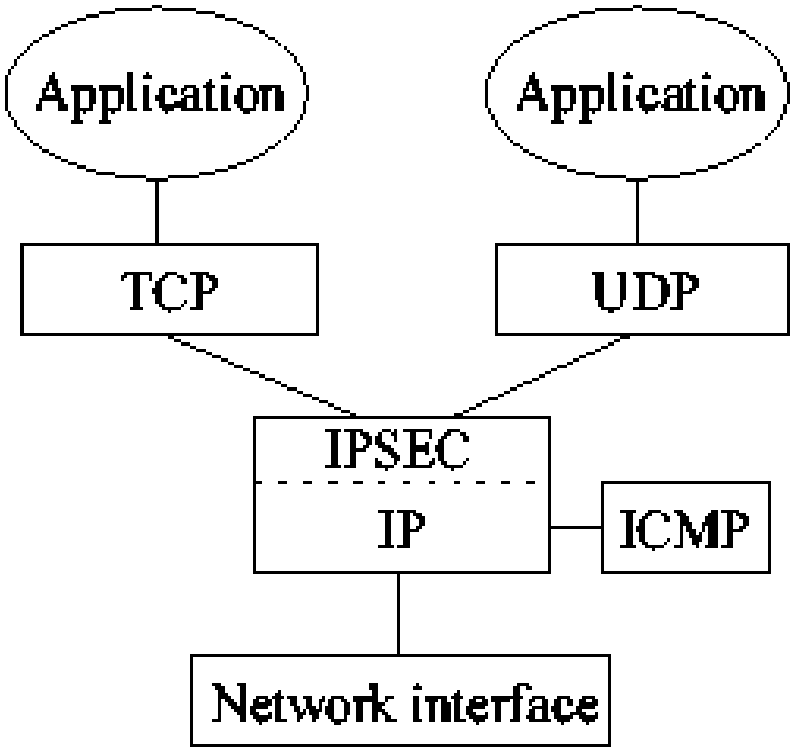
- Confidentialité
- Authentification
- Garantie d'integrité



=> Tous ces 3 conditions sont nécessaire pour une connexion veritablement protegée!

  - p.e. man-in-the-middle attack

1.a) IPsec dans le système de couches



- Couches additionelles ajoutées entre *liaisons* et *réseau*

  => protection de tous protocoles et données basées sur IP

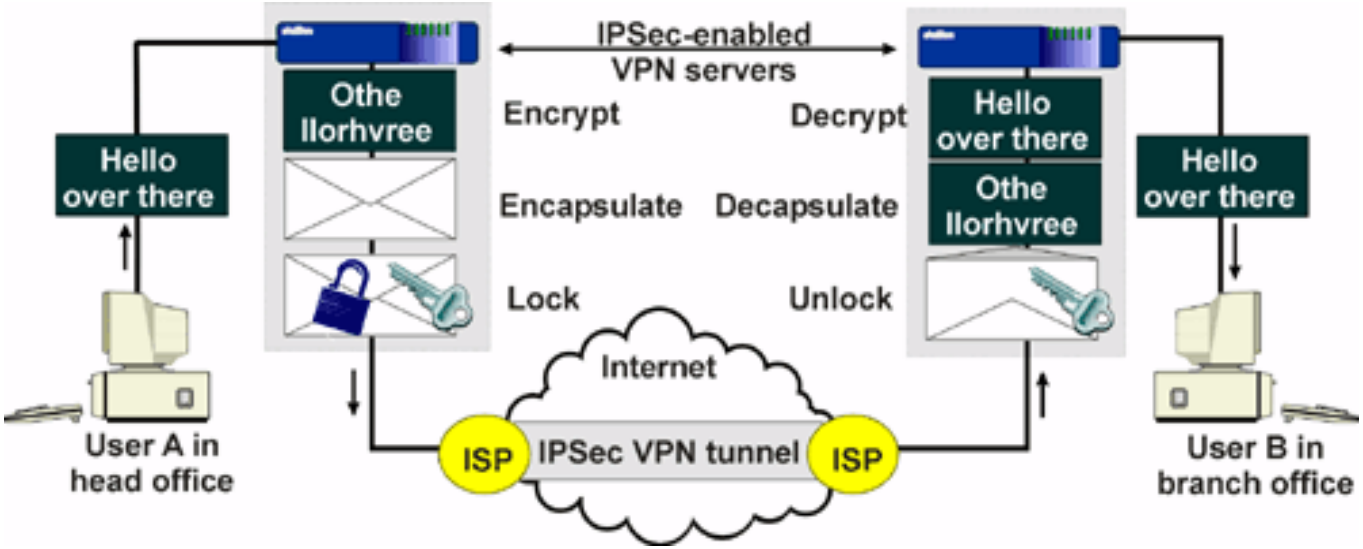
- addition optionelle pour IPv4, obligatoire pour IPv6

1.b) IPsec <=> procoles de la couche application

- Avantages de IPsec par rapport aux protocoles protegés de la couche application (ssh, https):
  - transfer de clés, identifications pas necessaire pour tous les applications
  - possibilité de protéger des applications de sécurité «faible» (p.e. Windows SMB)
  - programmeurs d'applications pas spécialistes
  - réductions des points d'attaque contre de protocoles spécifiques
- => Protection supérieure

1.c) Application primaire: VPNs

- VPN: *Virtual Private Network* (Réseau privé virtuel)
- Tunnel Internet fortement chiffré au lieu de liens permanents coûteux



2.a) Internet Key Exchange (IKE)

- Utilisé pour negocier les algorithmes et les clés utilisées par les autres protocoles (AH/ESP)
- Pour s'accorder sur une clé, on utilise l'algorithme de Diffie-Hellman (algorithme de clé asymétrique)

2.a) Internet Key Exchange (IKE)

Security Parameter	Example value
SPI (Security Parameter Index)	2916
AH Algorithm	MD5
AH Algorithm Mode	Keyed
AH Transform	RFC 1828
AH Key(s)	a 128 bit MD5 key
AH Mode	Entire Datagram
ESP Algorithm	DES
ESP Algorithm Mode	CBC
ESP Transform	RFC 1829
ESP Key(s)	a 56 bit DES key
ESP Mode	Transport
ESP Synch/Init Vector Size	64
Lifetime	an absolute time in Unix Time format
IPSO/CIPSO Sensitivity Label	Nuclear/Classified

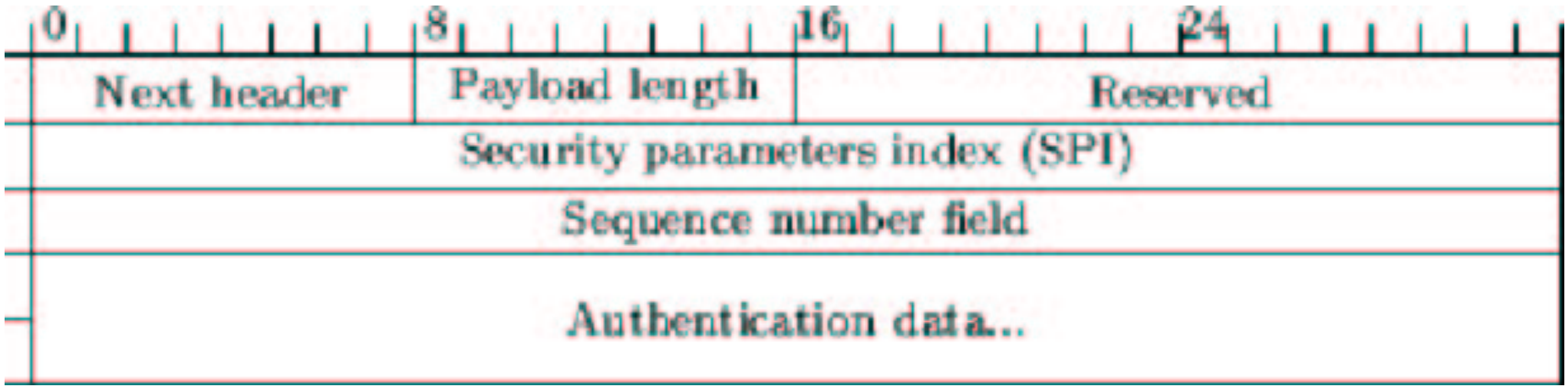
- paramètres des protocoles sont stockés dans une entité appelé *Security Association* (SA)
- SA n'est valable que dans une sens unique => deux SAs par communication mutuelle

2.b) Authentication Header (AH)

entête d'authentification

- fournit authentification de l'emetteur
- fournit garantie de l'intégrité du paquet
- securité contre man-in-the-middle attack, mais donnés inclus dans le paquet restent visibles
- algorithmes utilisés: hashing algorithms avec clés (HMAC)

2.b) Authentication Header (AH)

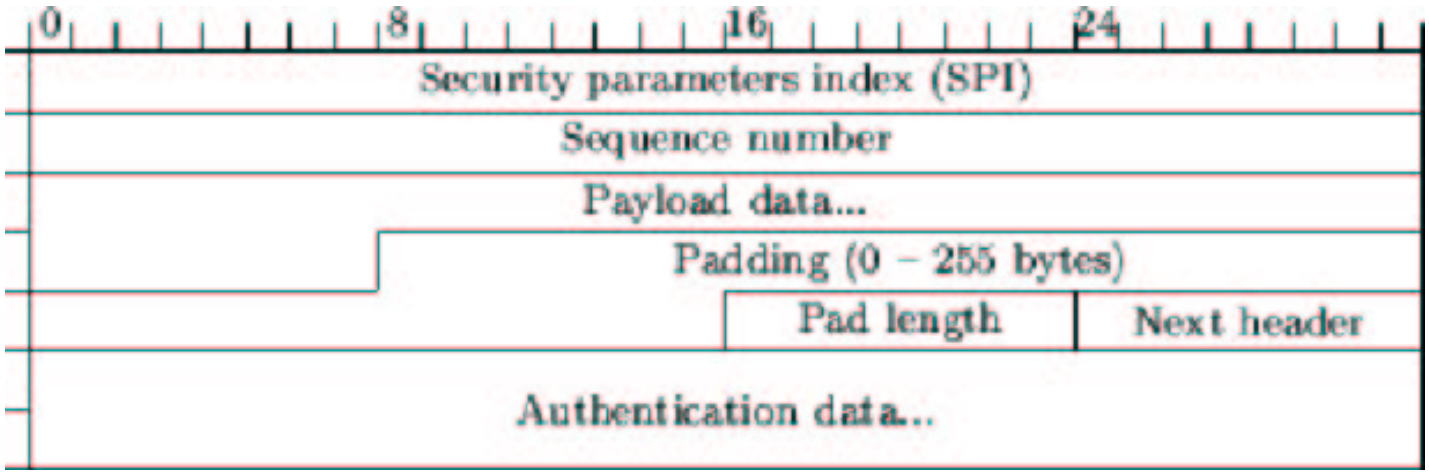


les champs de l'entête d'authentification

2.c) Encrypted Security Payload (ESP)

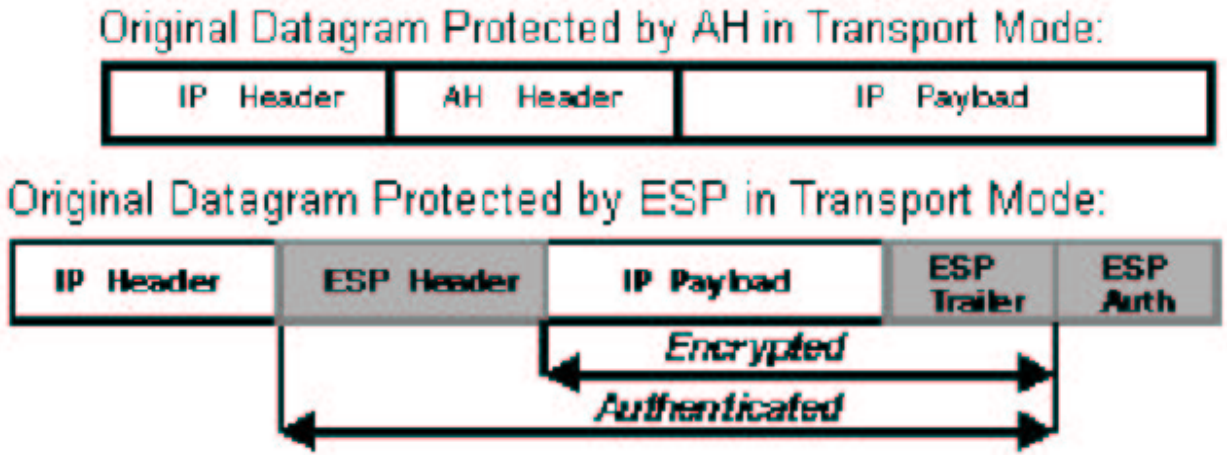
- chiffrage des donnés inclus dans le message
- authentification et garantie de l'intégrité comparable à l'AH, mais pas pour le paquet entier
- securité dependant de l'algorithme utilisé (p.e. DES ou 3DES)
- modes d'ESP:
  - chiffrage sans authentification (p.e. utilisé avec AH)
  - chiffrage et authentification

2. c) Encrypted Security Payload (ESP)



les champs de l'entête et de l'appendice d'ESP

3. Modes d'opérations: transport versus tunnel



Mode transport:

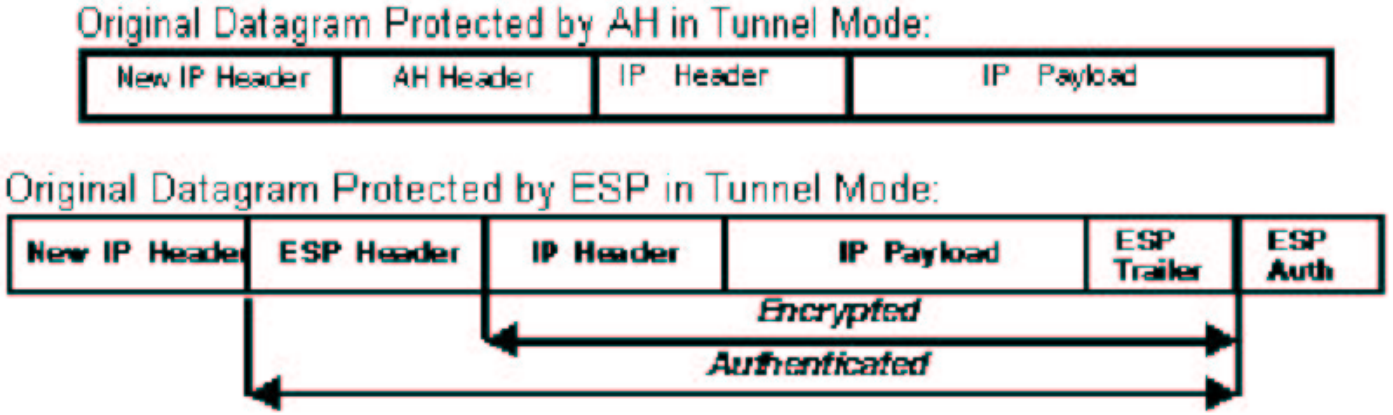
- utilisé dans des LANs insécures (p.e. Wireless LAN)

3. Modes d'opération: transport versus tunnel

Mode transport:

- advantages:
  - paquets plus petits, degré d'efficacité plus grand
- inconvenients:
  - tout les routeurs doivent connaisser les adresses d'emetteur et de recepteur (adresses privés)
  - utilisation de NAT pas possible
  - problème de performance avec des machines faibles

3. Modes d'opération: transport versus tunnel



Mode tunnel:

- paquet entier regardé comme donné et inclus dans un nouveau paquet IP
- utilisé pour connecter des LANs par un lien publique (p.e. Internet)

3. Modes d'opération: Transport versus Tunnel

Mode tunnel

- avantages:
  - ESP: chiffrage pour le paquet entier
  - adresses des machines pas visible en trajet
  - possibilité de connecter des réseaux privés par l'Internet
- inconvenients:
  - pas de sécurité entre les machines et le gateway
  - paquets plus lourds
  - diagnose des problèmes dans le réseau plus difficile

4.) Limitations et problèmes

- Dans la couche réseaux, pas de distinction entre donnés «secrets» ou non
  => overhead inutile
- standard assez vague, beaucoup de fonctionnalité optionelle, comprennant des protocoles démodés (DES)
  => problèmes de compatibilité
- implementations errones et pas complêtes (Win2000, FreeSWAN/Linux)
- complexe à installer et administrer

Conclusion

- Malgré les possibilités plus vastes, IPsec est utilisé aujourd'hui presque exclusivement pour protéger des VPNs, avec Hardware dédié

- L'avenir:
  - introduction d'IPv6
  - implementations plus mûres
- => diffusion plus forte semble probable

Questions?