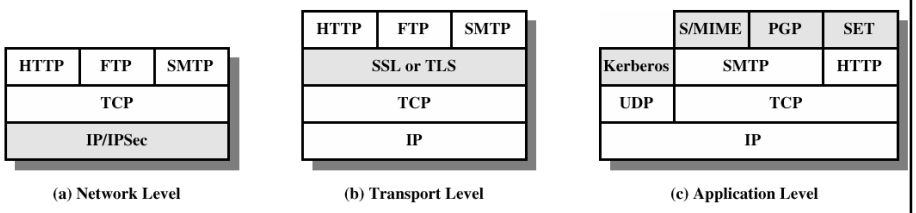
Protocoale de nivel aplicaţie:

IPSec

Comparaţie



- La ce nivel al stivei TCP/IP se poate implementa un protocol de securitate?

Securitatea IPv4

- IPSec
- conectivitate între filiale “peste” Internet
- *remote access* prin Internet
- securitatea *e-commerce*

IPSec - aspecte

2 variante:

- Authentication Header - AH - *doar autentificare*

(nu şi criptarea conţinutului pachetului)
algoritmi: HMAC-MD5, HMAC-SHA1
HMAC = *Hashed Message Authentication Code*

- Encapsulated Security Payload - ESP - *criptarea conţinutului pachetului*

algoritmi: DES, 3DES, AES, IDEA ...

- RFC 2401,2402,2406,2408

Asocieri de securitate (SA)

- Relaţie unidirecţională între exp. şi destinatar.
- permite negocierea params. de securitate între E şi D
- Pt relaţie bidirecţională - sunt necesare două asocieri
- Trei parametri identifică un SA
  - Security Parameter Index - SPI (identificator unic)
  - IP sursă, IP destinaţie
  - Security Protocol Identifier - AH sau ESP
- SA negociat între E şi D folosind protocolul IKE = *Internet Key Exchange*

Parametri SA

- Protocol AH/ESP
- Algoritmi criptografici utilizaţi
- cheile, IV...
- durata de viaţă a asociaţiei
- adresa capătului opus
- nivelul de senzitivitate al datelor

Bază de date SA

Se crează o bază de date cu:

- Parametrii SA precedenţi
- Contor de numere de secvenţă
- Path MTU

În baza de date a receptorului, o intrare este identificată de:

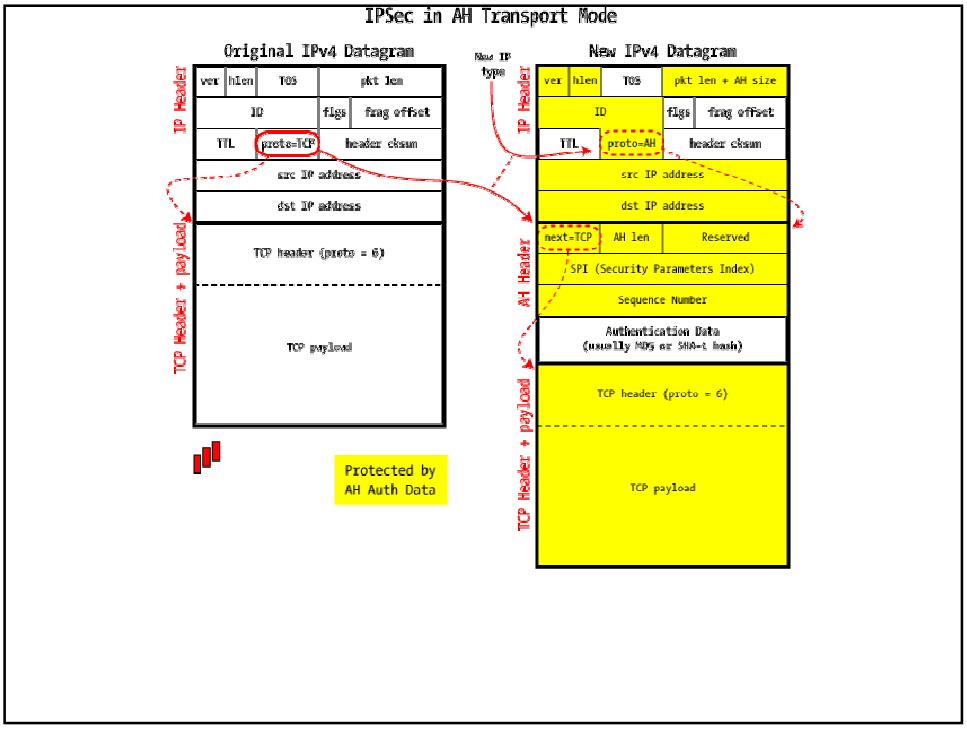
- SPI (Security Parameters Index), indexul SA în baza de date de SA-uri a receptorului, inserat de emiţător
- adresa IP destinaţie
- Security Protocol Identifier: AH/ESP

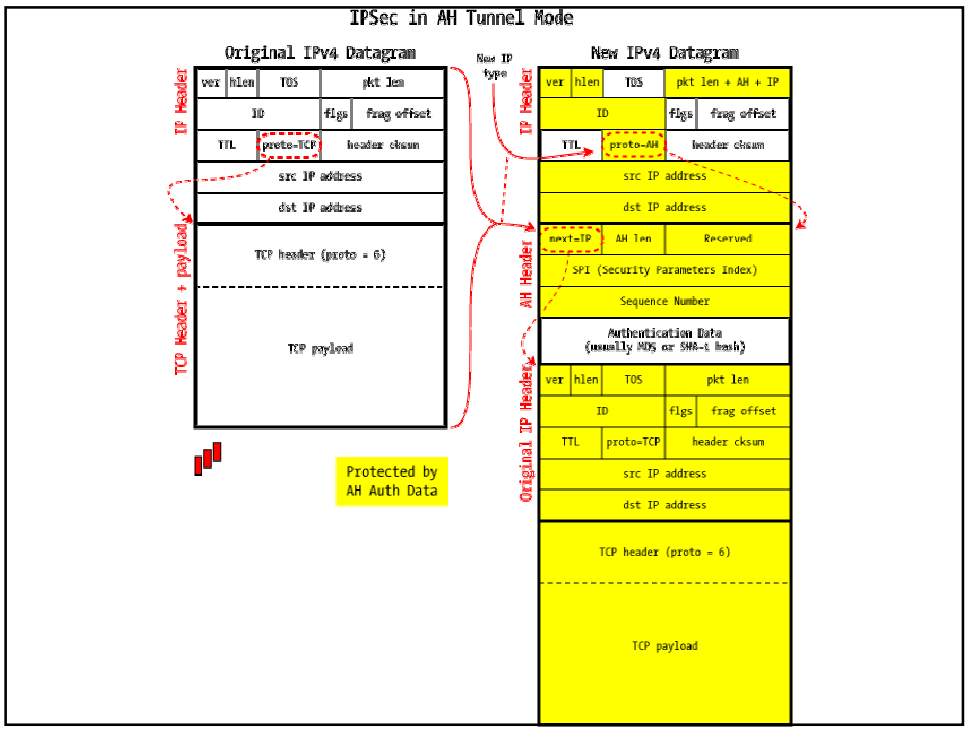
SA - conexiune ?

- IP este conectionless;
- parametrii SA şi se negociază la început (protocol, chei, etc) → similar cu negocierea unei conexiuni
- parametrii rămîn activi pe toată durata "conexiunii"
- deci: IPSec este practic connexion-oriented datorită existenţei SA

Moduri AH sau ESP: Transport şi Tunel

- Modul Transport
  - Protecţie pt nivele superioare, ex. TCP/UDP
  - Se extinde la partea de date a pachetului IP
  - Headerul IP nu este inclus
  - Capăt la capăt
- Modul Tunel
  - Protecţie pt. pachetul IP în întregime
  - Pachetul vechi este încapsulat într-unul nou
  - Nici un ruter nu examinează pachetul interior
  - Poate avea adrese IP sursă şi destinaţie diferite
  - Poate fi implementat în firewall



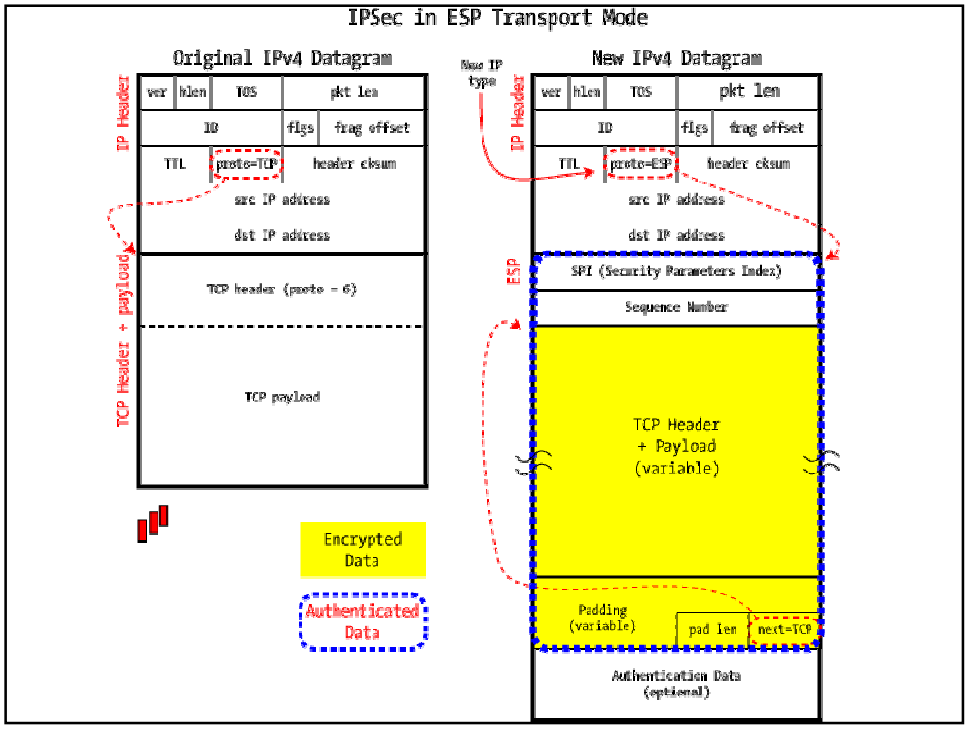


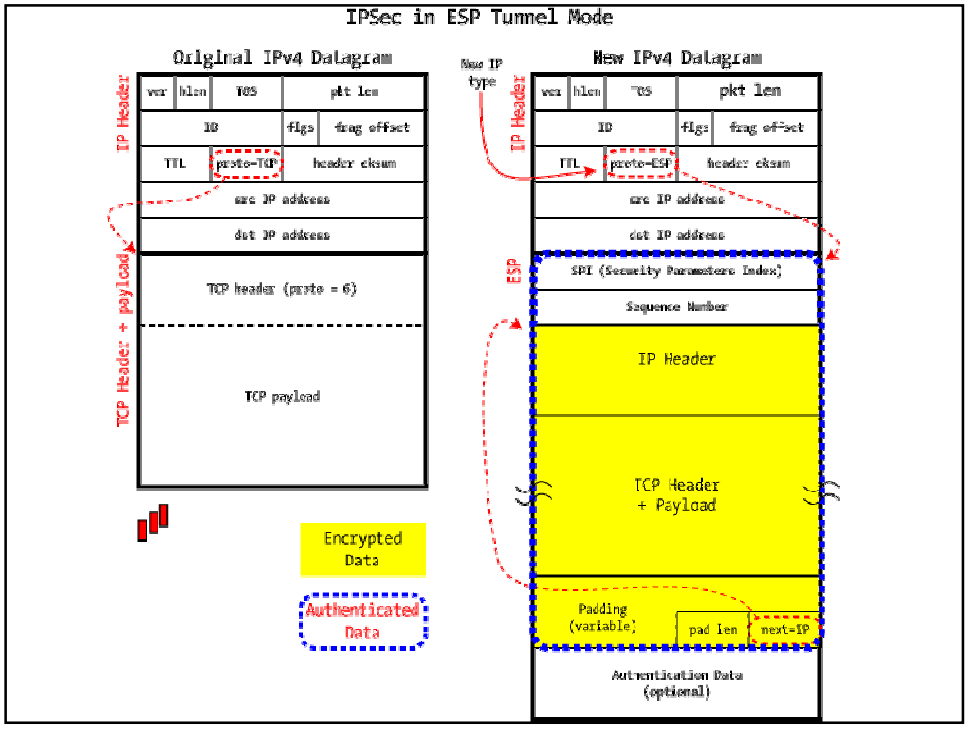
Observaţii

- Authentication data: se face un SHA-1 (sau MD5) al (pachetului+cheia), numit HMAC
- Se foloseşte SHA-1 sau MD5 şi cheia comună, negociată iniţial, în locul unui sistem cu chei publice, din considerente de viteză - IPSec se aplică fiecărui pachet IP, nu doar unei faze iniţiale de stabilire a conexiunii !
- Contorul numerelor de secvenţă este unic chiar şi pt pachete retransmise; astfel se evită atacurile de tip *replay*

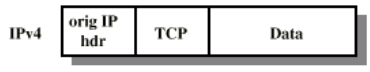
IPSec şi NAT

- OBS: AH protejează (zona galbenă) cîmpurile de adresă IP sursă şi dest
- NAT modifică aceste cîmpuri
- → IPSec/AH incompatibil cu NAT
- IPSec/ESP compatibil cu NAT căci headerul nu este afectat de ESP

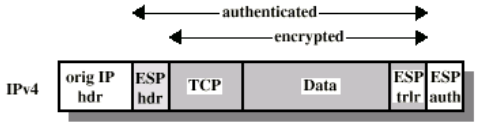




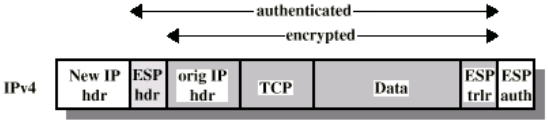
Utilizarea ESP



(a) Original IP Packet



(b) Transport Mode



(c) Tunnel Mode

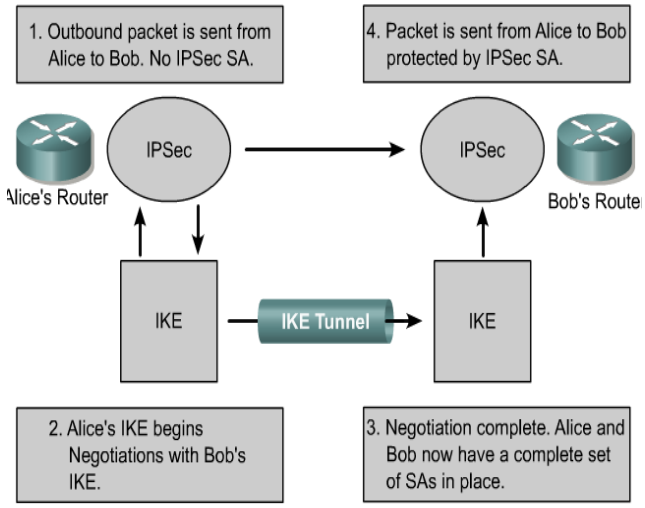
Comparaţie AH/ESP

- AH există pentru că a fost dezvoltat primul; prin dezvoltarea ESP care face autentificare+ criptare, AH devine mai puţin util şi probabil va fi abandonat în viitor
- La ESP, HMAC se plasează la sfîrşitul pachetului → avantaj la calculul *on-the-fly* în timpul transmiterii pachetului → spor de viteză (din acelaşi motiv FCS la Ethernet se pune la sfîrşit)
- Singurul dezavantaj ESP: nu se autentifică şi headerul pachetului IP, ca la AH

Managementul Cheilor

- Manual: cheile sînt configurare manual la cele 2 capete ale legăturii
- Automat: IKE (ISAKMP Key Exchange)
  - port 500/UDP
  - bazat pe ISAKMP/Oakley
    - ISAKMP=Internet Security Association Key Management Protocol
    - Protocol de determinare a cheilor Oakley
    - Protocol pentru asocierile de securitate şi management al cheilor ISAKMP

Utilizarea IKE în IPSec



Bibliografie

[1] William Stallings, *Data and Computer Communications,* Capitolul 18

[2] Steve Friedl's Unixwiz.net Tech Tips, *An Illustrated Guide to Ipsec*