IPsec – bezpieczeństwo sieci komputerowych

Bartłomiej Świercz

Katedra Mikroelektroniki i Technik Informatycznych

Łódź, 18 maja 2006

Wstęp

Jednym z najlepiej zaprojektowanych protokołów w informatyce jest protokół IP o czym świadczy fakt, że jest używany nieprzerwanie od przeszło 20 lat w środowisku komputerowym, które niesłychanie szybko się zmienia.

Pomimo faktu, że protokół IP został zaprojektowany w celu przetrwania ataku nuklearnego, to nie zapewnia on podstawowych wymagań stawianych nowoczesnym siecią komputerowym jakim są bezpieczeństwo i poufność przesyłanych danych.

Przez wiele lat jedyną możliwością zapewnienia bezpiecznych połączeń w sieci Internet było używanie protokołów wyższych warstw (PGP, SSL, SSH).

IP Security — IPsec

IPsec jest zbiorem protokołów, których celem jest zapewnienie integralności oraz poufności przesyłanych danych. Prace nad IPsec rozpoczęła IETF w 1992 roku.

Integralność Integralność protokołu oznacza możliwość wykrycia zmian wprowadzonych do przesyłanych danych wraz z nagłówkami. Zmiany te mogą być przypadkowe lub celowe. Mechanizm ten opiera się na funkcjach skrótu, które w przeciwieństwie do funkcji sum kontrolnych (IP i TCP) dają jednoznaczną informację o integralności pakietu.

Poufność Poufność oznacza, że nie możliwe będzie odczytanie wiadomości bez znajomości klucza, który został użyty do ich zaszyfrowania.

IPsec — założenie techniczne

Ważną cechą protokołu IPsec jest jego przezroczystość dla warstw wyższych modelu ISO/OSI. Przezroczystość realizowana jest poprzez enkapsulację pakietów.

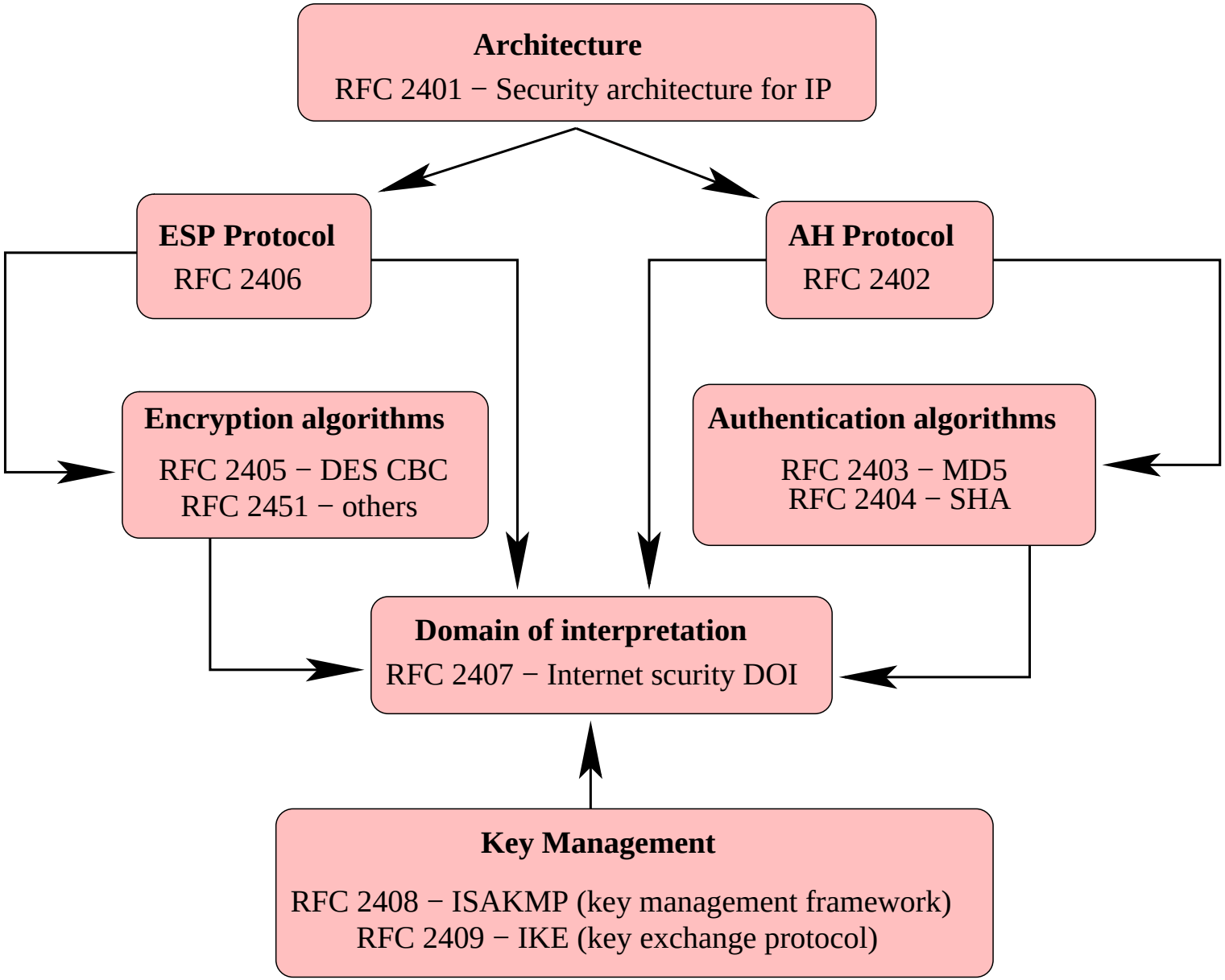
- Szyfrowanie informacji.
- Kontrola integralności.
- Autentyfikacja węzłów nawiązujących połączenie.
- Mechanizm anti-replay.
- Przezroczystość.

IPsec — wady proponowanego rozwiązania

Podstawową wadą IPsec jest jego duża złożoność i częsta nadmiarowość stosowanych rozwiązań. Wady te nie wynikają z błędów projektowych lecz z polityki wielu państw dotyczącej kryptografii.

- Protokół AH kontra ESP.
- Tryb tunelowy kontra tryb transportowy.
- Różne metody kryptografii (MD5, SHA, DES, 3DES, AES . . .).
- IKE kontra manualna konfiguracja.
- Główny tryb pracy kontra agresywny tryb pracy.

Architektura IPsec



Architektura IPsec — AH i ESP

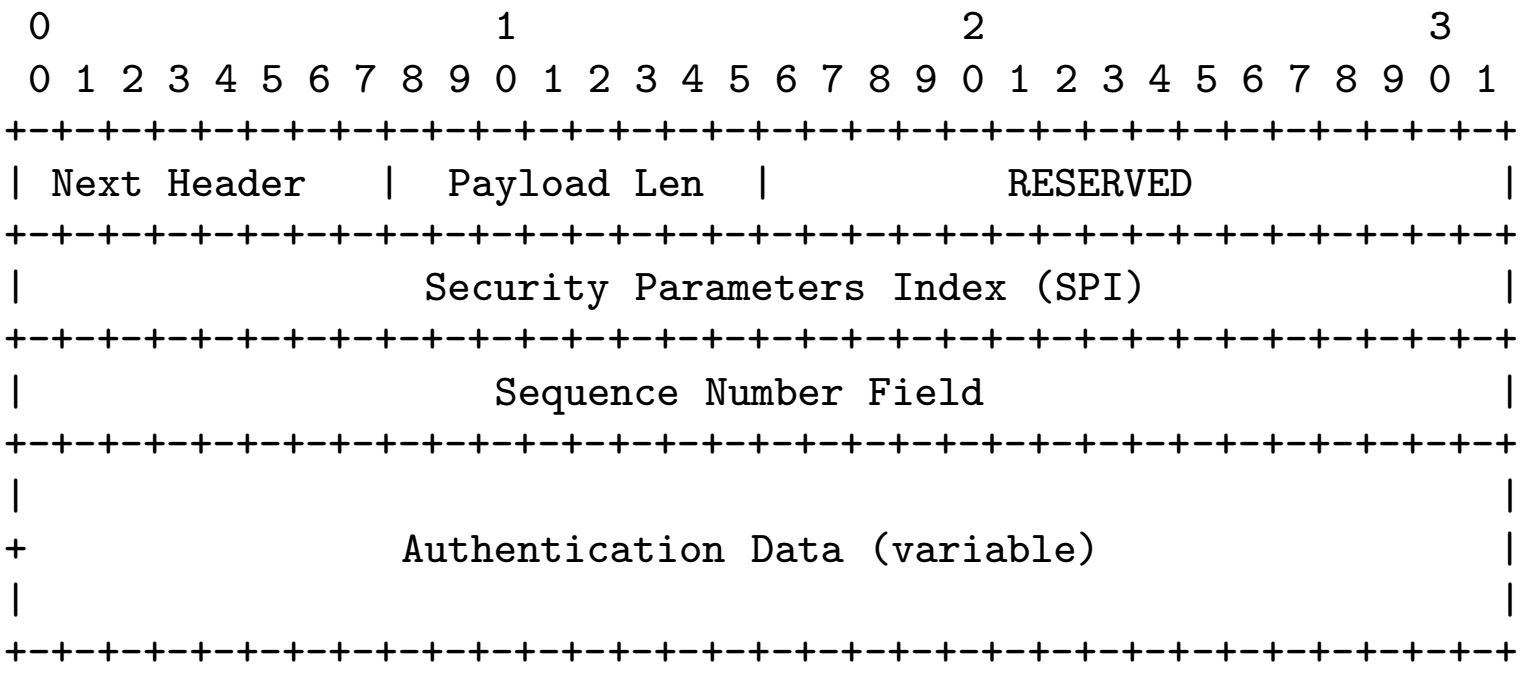
Protokół IPsec związany jest z protokołem IP. Oznacza to, że pakiety poruszające się w sieci to są zawsze pakiety IP, a zaraz za nim są enkapsulowne protokoły bezpieczeństwa takiej jak AH lub ESP.

Protokół AH Autentication Header zapewnia integralność zarówno eknkapsulowanych danych jaki części nagłówka IP, która nie ulega zmianie podczas przesyłania przez sieć. Do określenia integralność danych używa się kryptograficznych funkcji skrótu takich jak: MD-5, SHA-1 czy RIPEMD-160.

Protokół ESP Encapsulation Security Payload protokół zapewnia oprócz integralności również szyfrowanie danych. W przeciwieństwie do protokołu AH, protokół ESP nie zapewnia integralnej ochrony nagłówka IP.

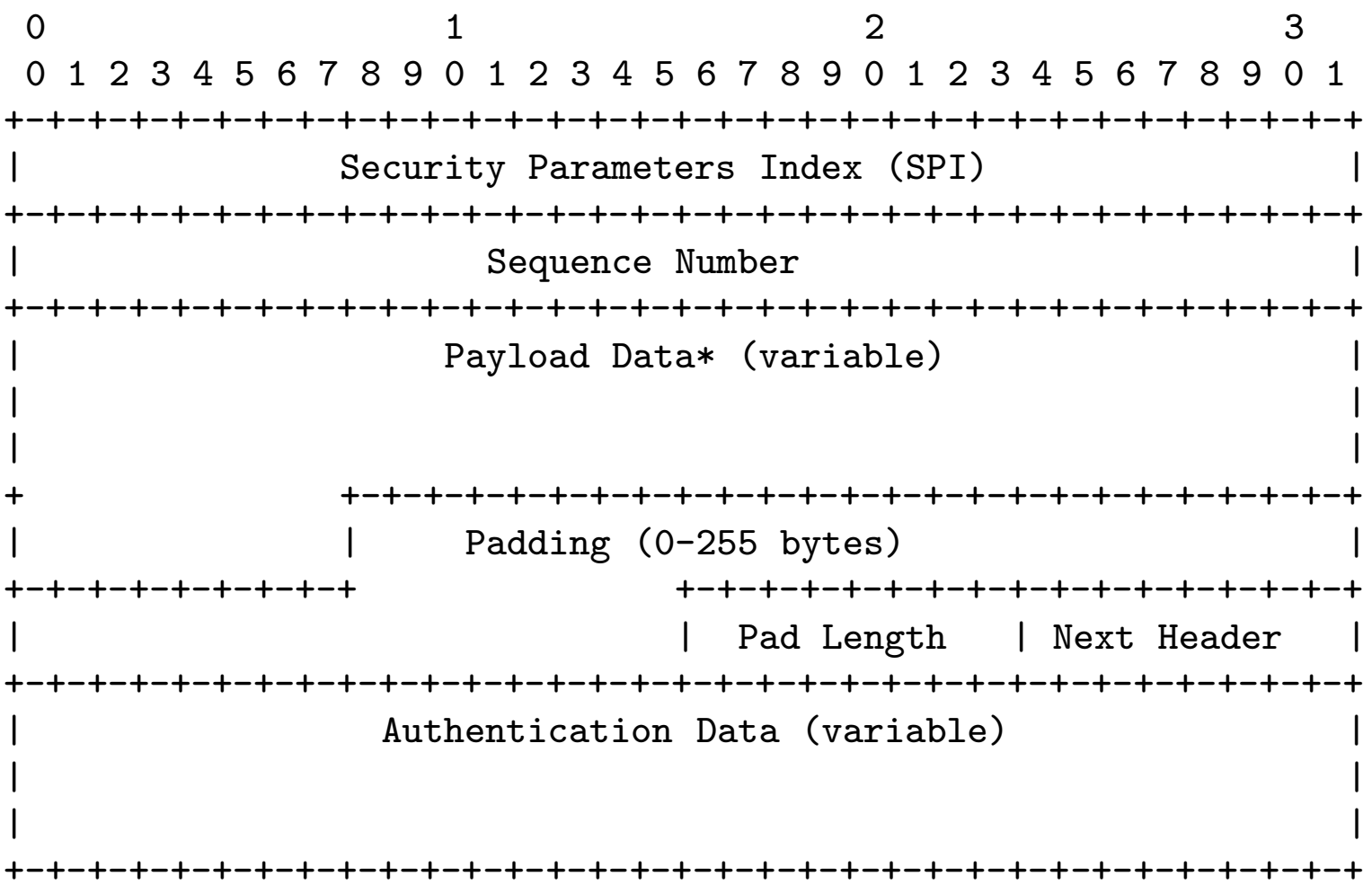
Nagłówek AH

Zgodnie z dokumentem RFC 2402 nagłówek protokołu AH wygląda następująco:



Nagłówek ESP

Zgodnie z dokumentem RFC 2406 nagłówek protokołu ESP wygląda następująco:



Tryb transportowy i tunelowy

Zarówno protokół AH jak i ESP może być użyty do trybu pracy transportowego lub tunelowego.

Pakiet IP

```
+----+-----+--------------------
| IP | TCP | dane użytkownika...
+----+-----+--------------------
```

Tryb transportowy i tunelowy

Zarówno protokół AH jak i ESP może być użyty do trybu pracy transportowego lub tunelowego.

Tryb transportowy

```
+----+-----+=========================
| IP | ESP | TCP | dane użytkownika...
+----+-----+=========================
```

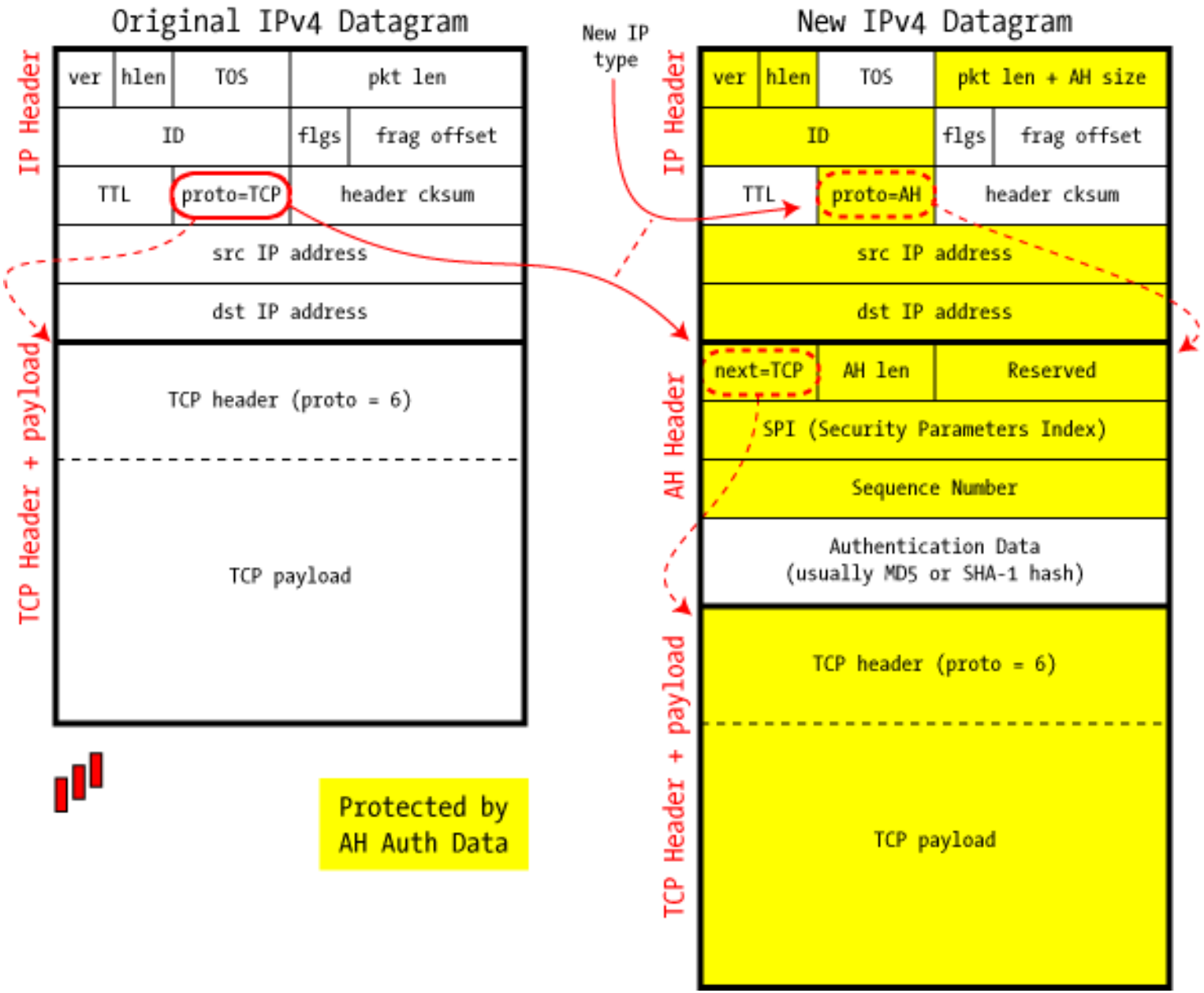
Tryb transportowy i tunelowy

Zarówno protokół AH jak i ESP może być użyty do trybu pracy transportowego lub tunelowego.

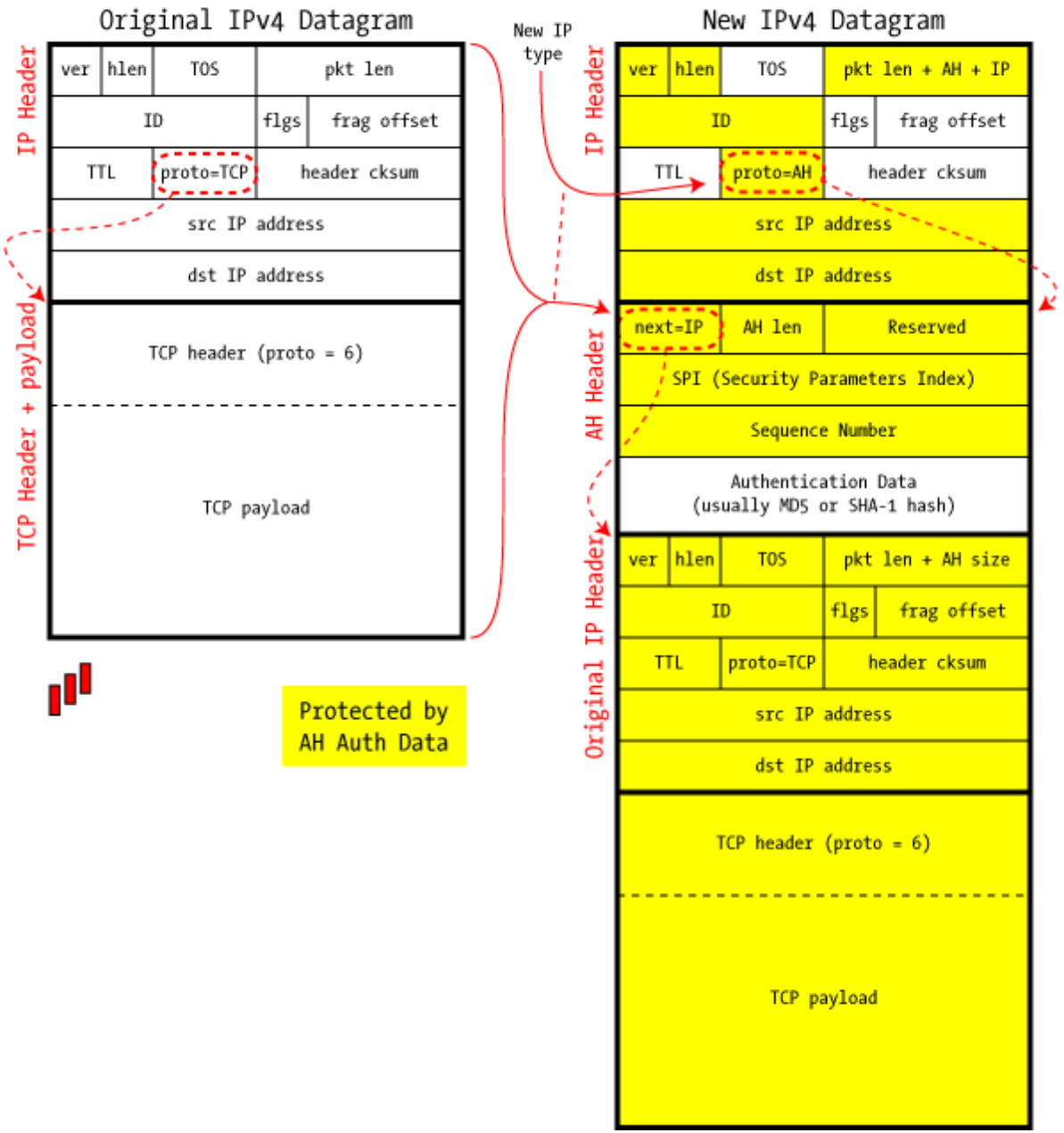
Tryb tunelowy

```
+-----+-----+==============================
| IPn | ESP | IP | TCP | dane użytkownika...
+-----+-----+==============================
```

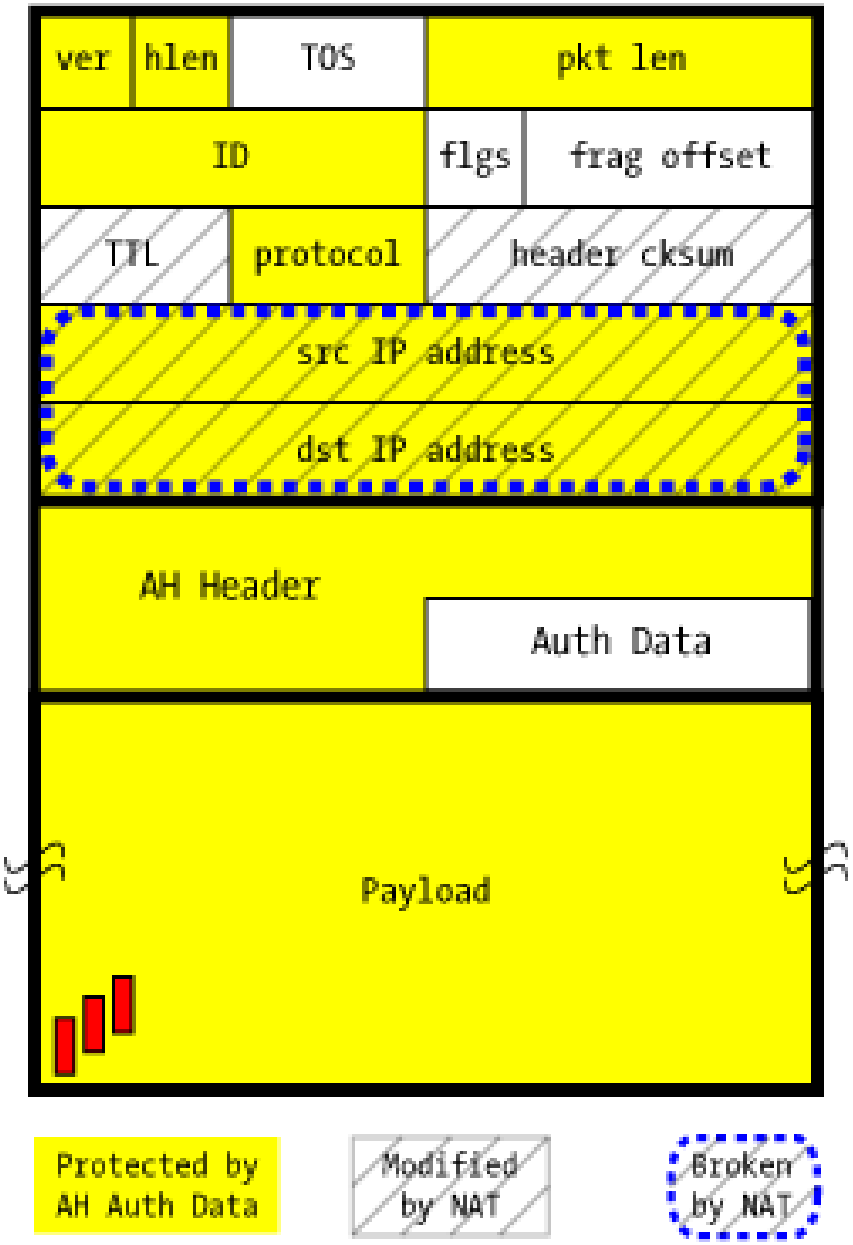
IPSec in AH Transport Mode



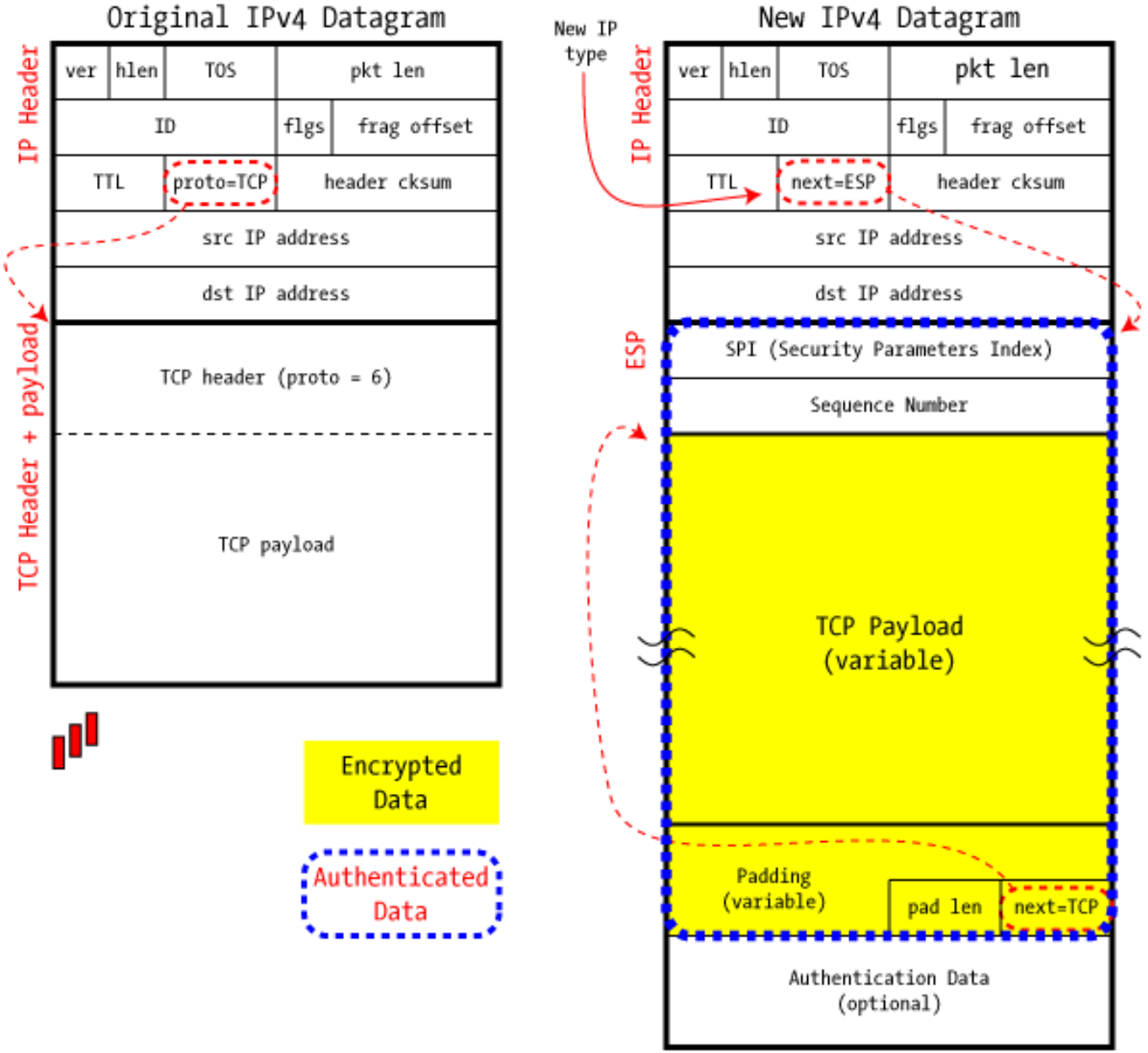
IPSec in AH Tunnel Mode



AH and NAT: Incompatible



IPSec in ESP Transport Mode



IPSec in ESP Tunnel Mode