An Introduction to the Tunneling Protocols

Alexandre Dulaunoy and various

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

10th February 2006

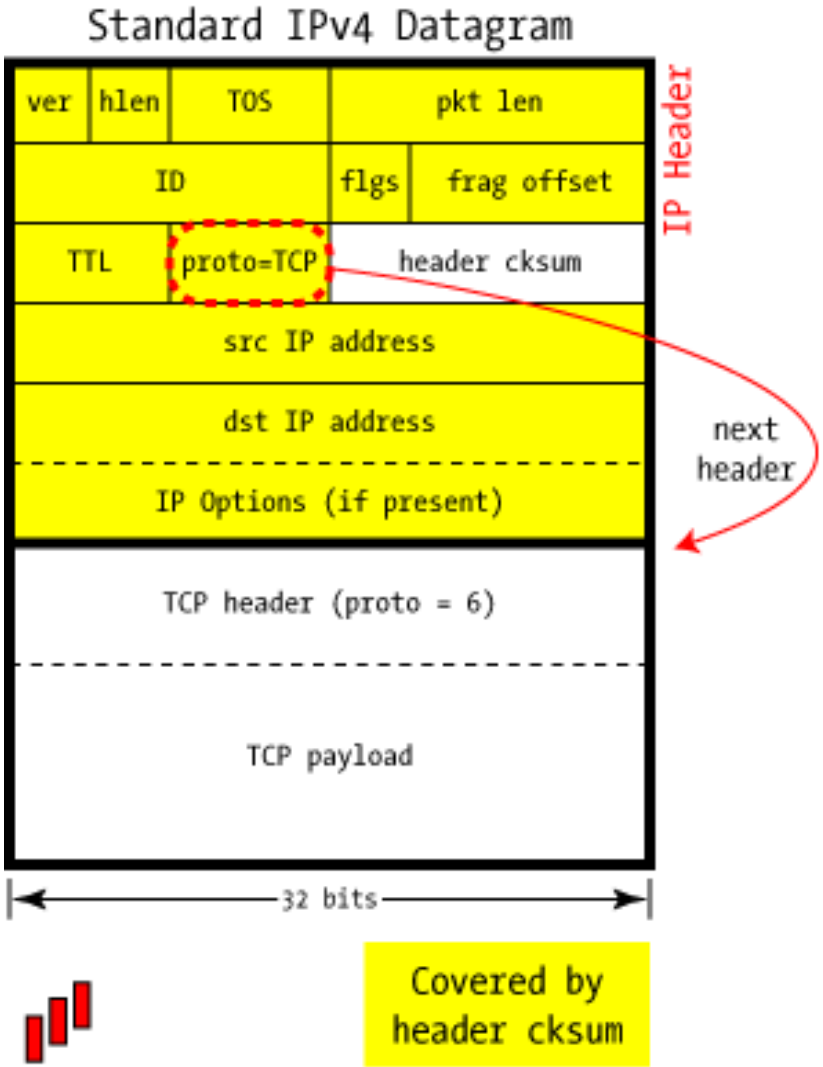
Definition of Tunneling Protocols

"A tunneling protocol is a network protocol which encapsulates one protocol or session inside another. Protocol A is encapsulated within protocol B, such that A treats B as though it were a data link layer. Tunneling may be used to transport a network protocol through a network which would not otherwise support it. Tunnelling may also be used to provide various types of VPN functionality such as private addressing."
e.g. : a transit network unsupporting a specific protocol (DECnet), the need to provide confidentiality and integrity for a specific network stream.

Types of Tunneling Protocols

- Stream oriented (e.g. SSL/TLS)
  - Encapsulation/Tunneling is done bytes per bytes.
- Datagram "packet" oriented (e.g. IPsec, PPP, PPTP)
  - Encapsulation/Tunneling is done per packet and packets are (often) standalone entities.

IP headers



proto : 4 (IPinIP), 47 (GRE), 50 (IPsec ESP), 51 (IPsec AH)

Generic Routing Encapsulation (GRE)

- described in RFC2784
- A first try to generalize and standardize the approach to encapsulate an arbitrary network layer protocol in another arbitrary network layer protocol.
- GRE header includes minimal information like an ether type.
- Cryptographic Integrity, Confidentiality is *not* provided by GRE.
- Various specific requirements are required when forwarding/decapsulating the packet. (TTL and alike)

PPTP

- described in RFC2637
- encapsulate network frame in PPP using the GRE tunneling protocol.
- use TCP port 1723 to manage the GRE tunnels. At least two sessions are required to establish one tunnel.
- Sessions are authenticated using MSCHAP-v2.
- Confidentiality and Integrity can be provided using MPPE (RFC3078) but various security flaws/issue exist.

IPsec

- IPsec a suite of tunneling (and non-tunneling) protocols to secure network connection.
- A (very) complex suite of protocols described by different RFCs.
- IPsec is a framework to build secure network connection (you can choose between the encryption, the various modes, authentication,...).

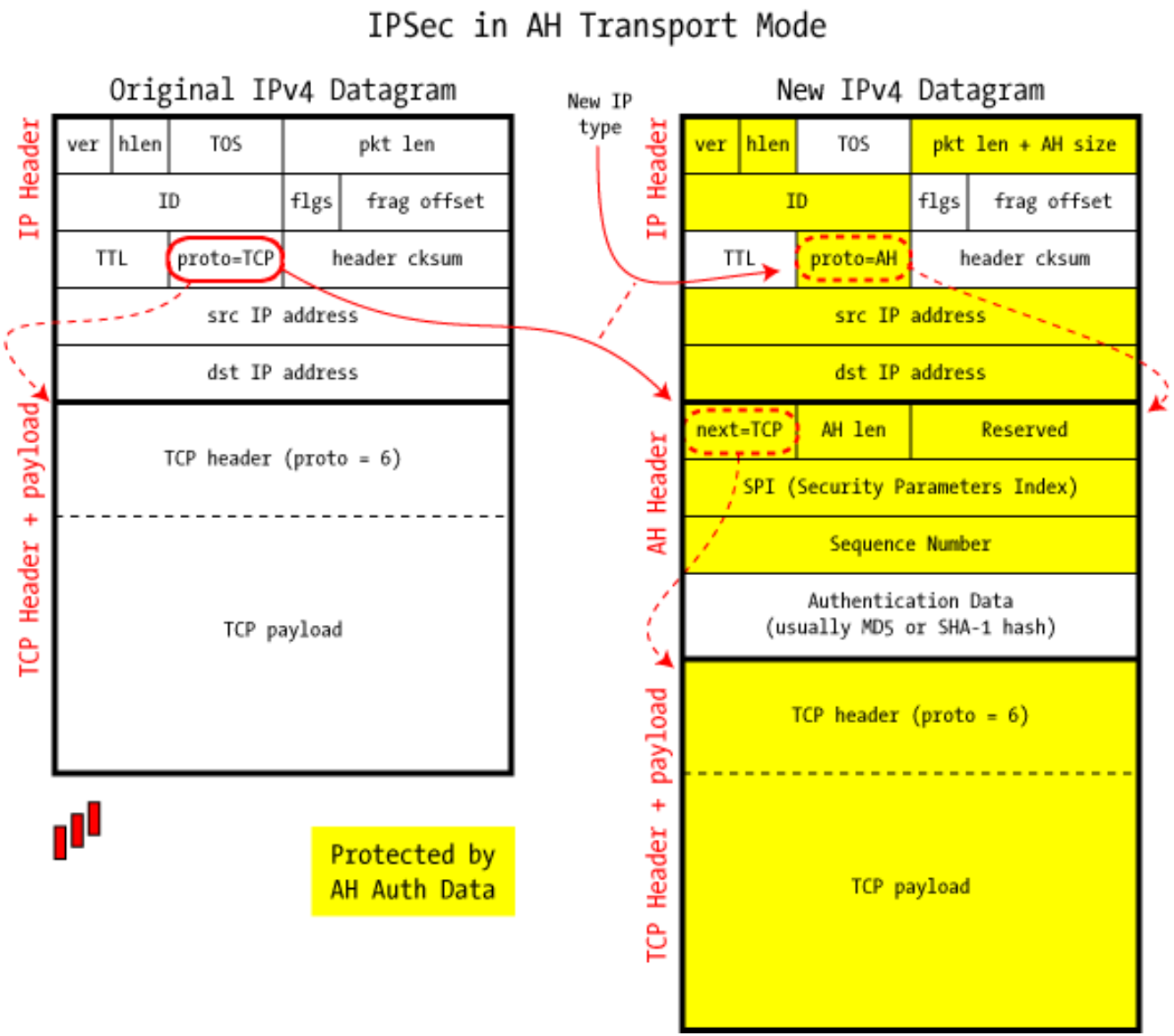
IPsec : the framework

- AH or ESP
  - Authentication mode (AH) or Encapsulation Security Payload (ESP). AH is just doing authentication but ESP is doing authentication and encryption.
- Tunnel mode or Transport mode
  - Transport Mode provides a secure connection between two endpoints (only IP payload) in Tunnel mode is the entire IP packets being encapsulated. (Tunnel or Transport mode ? ip type is always tunnel, the rest is transport...)
- Authentication and Encryption mode (AES+SHA1 ? AES+MD5)
  - Authentication calculates an Integrity Check Value (ICV) over the packet's contents, with crypto hash MD5 or SHA-1. The shared secret key used, and this allows the recipient to compute the ICV in the same way. by so authenticate both ends.

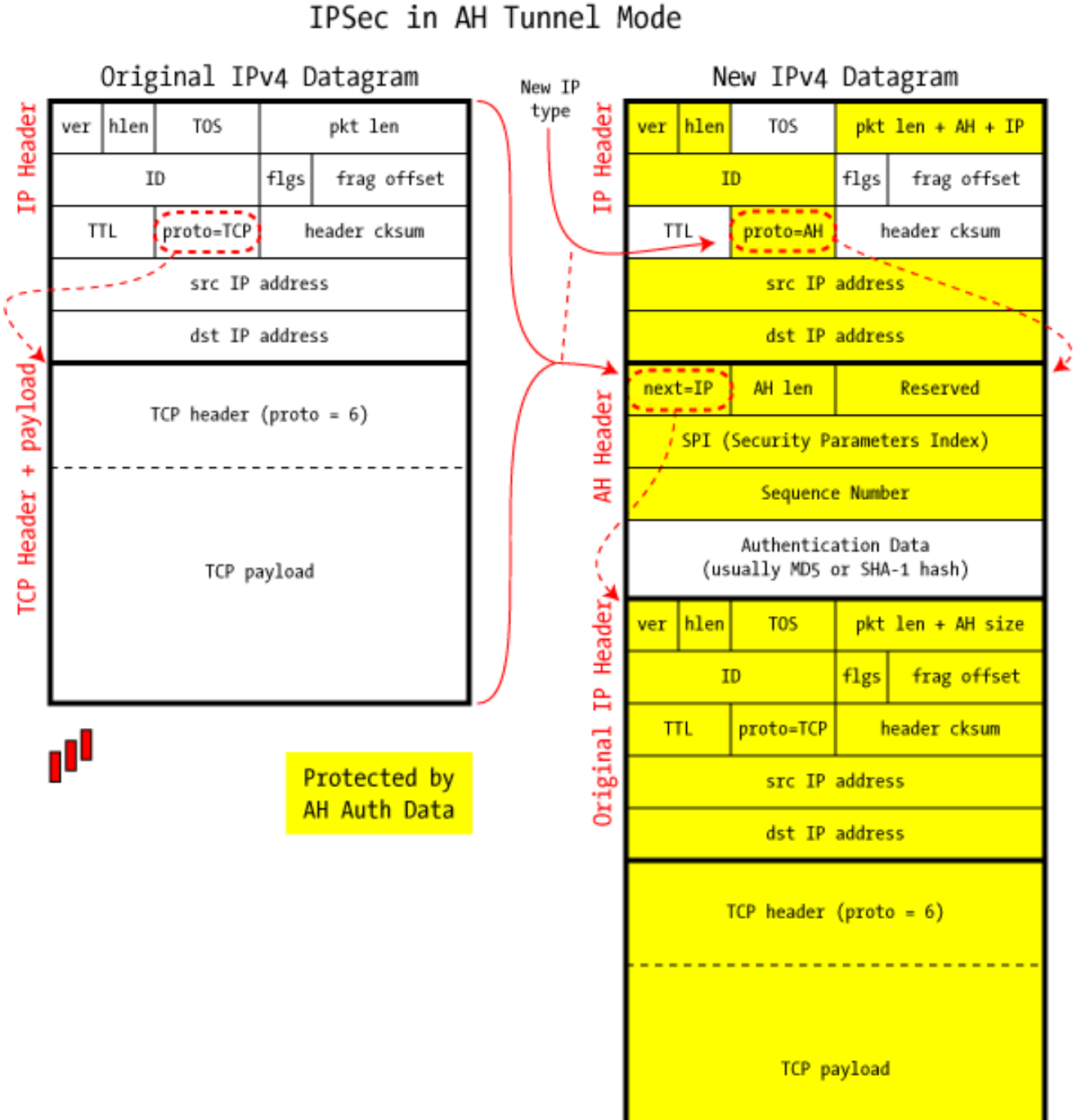
IPsec : the framework 2nd part

- IKE or manual keys
  - Various shared secrets (keys) must be shared between the various ends. You can manually set the various required keys by using a "second channel" to distribute the secrets. This can be very complicated with a large meshed vpn networks. IKE (a possible) key exchange is proposed in the IPsec framework in order to exchange info.
- Main mode or agressive mode
  - Main mode is a 6-ways initial exchange to setup the IKE key exchange. The main mode is secure but can generate compatibility issues between implementation. Agressive mode is simpler but somewhat weaker...

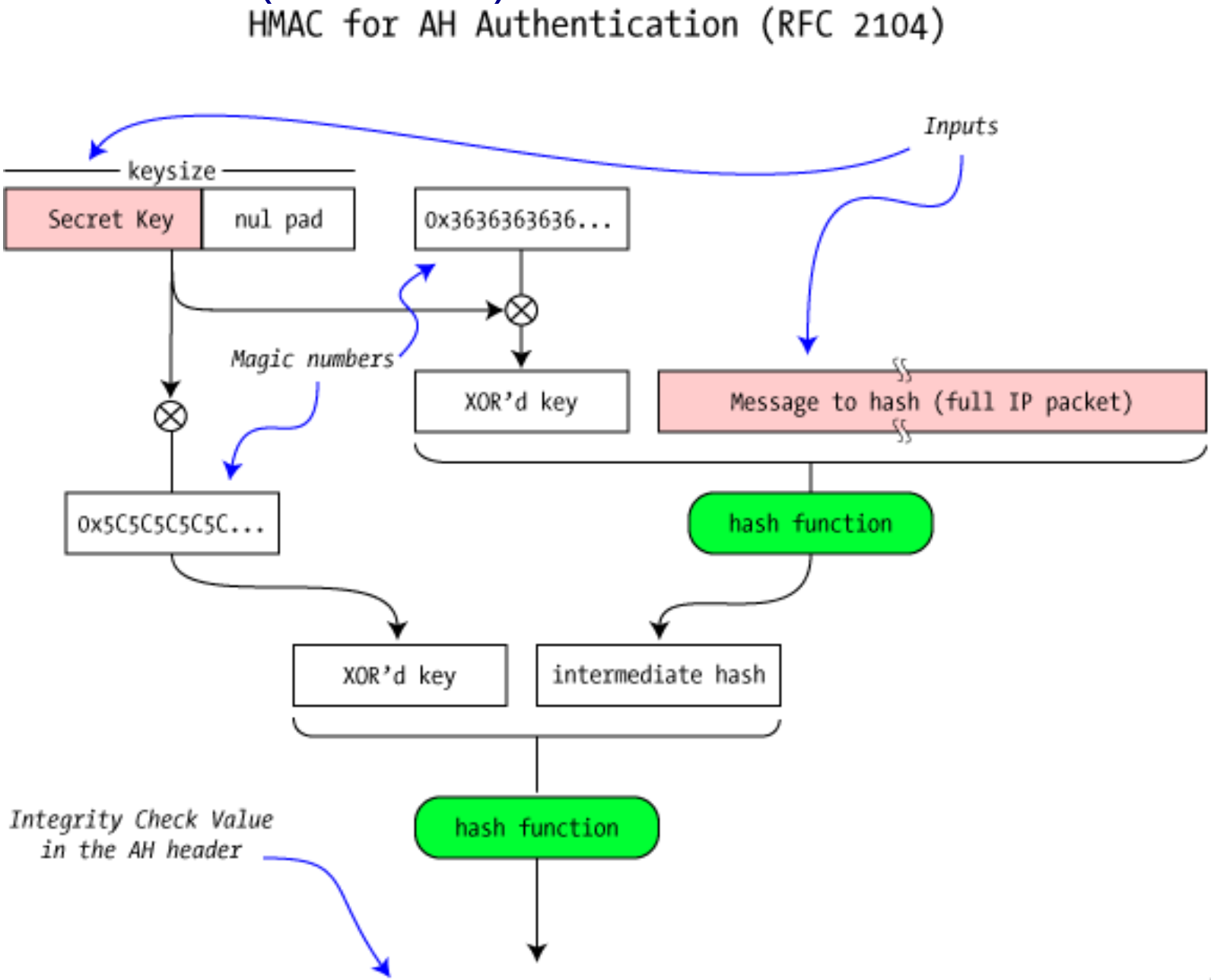
IPsec AH/Transport mode



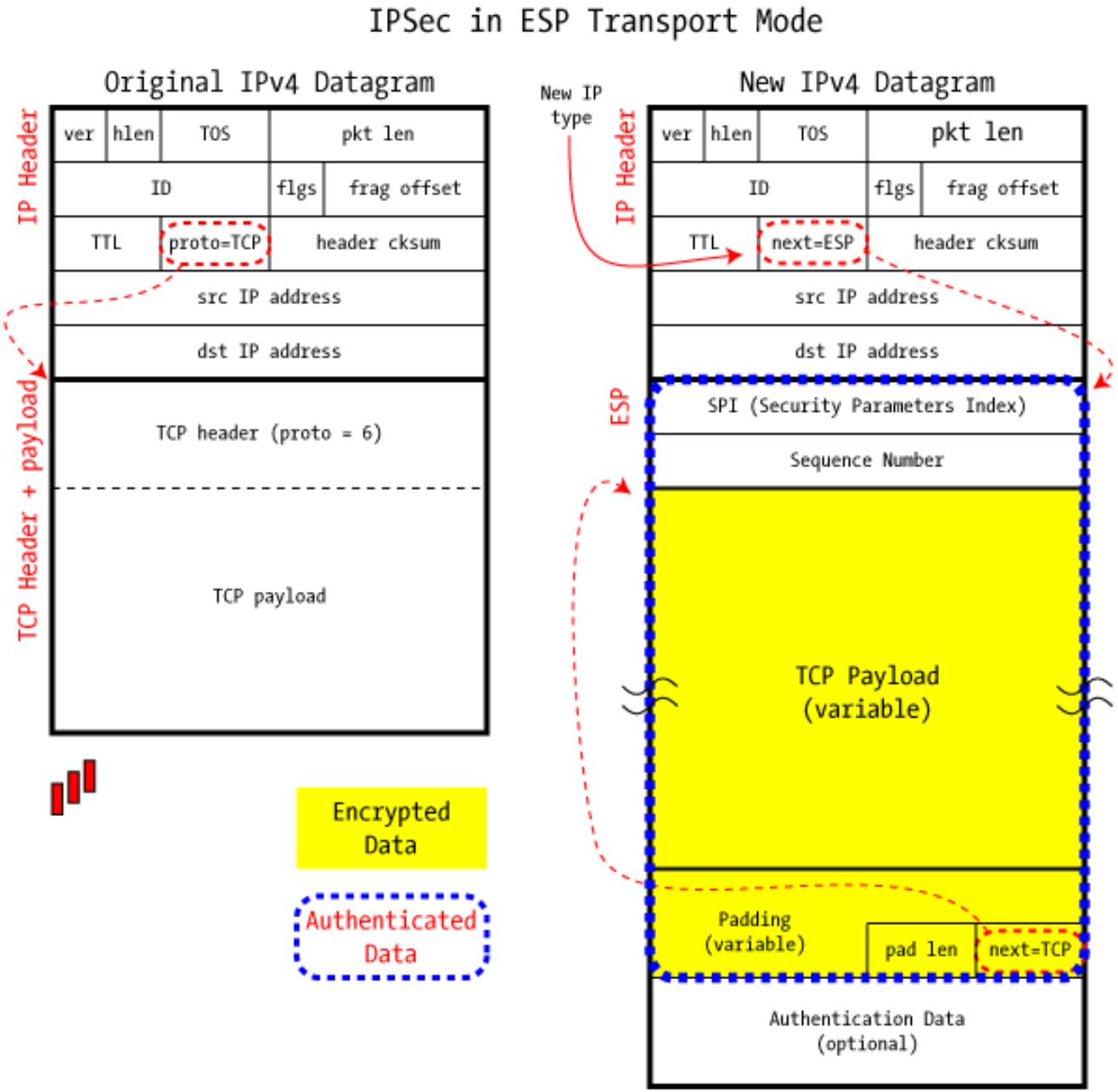
IPsec AH/Tunnel mode



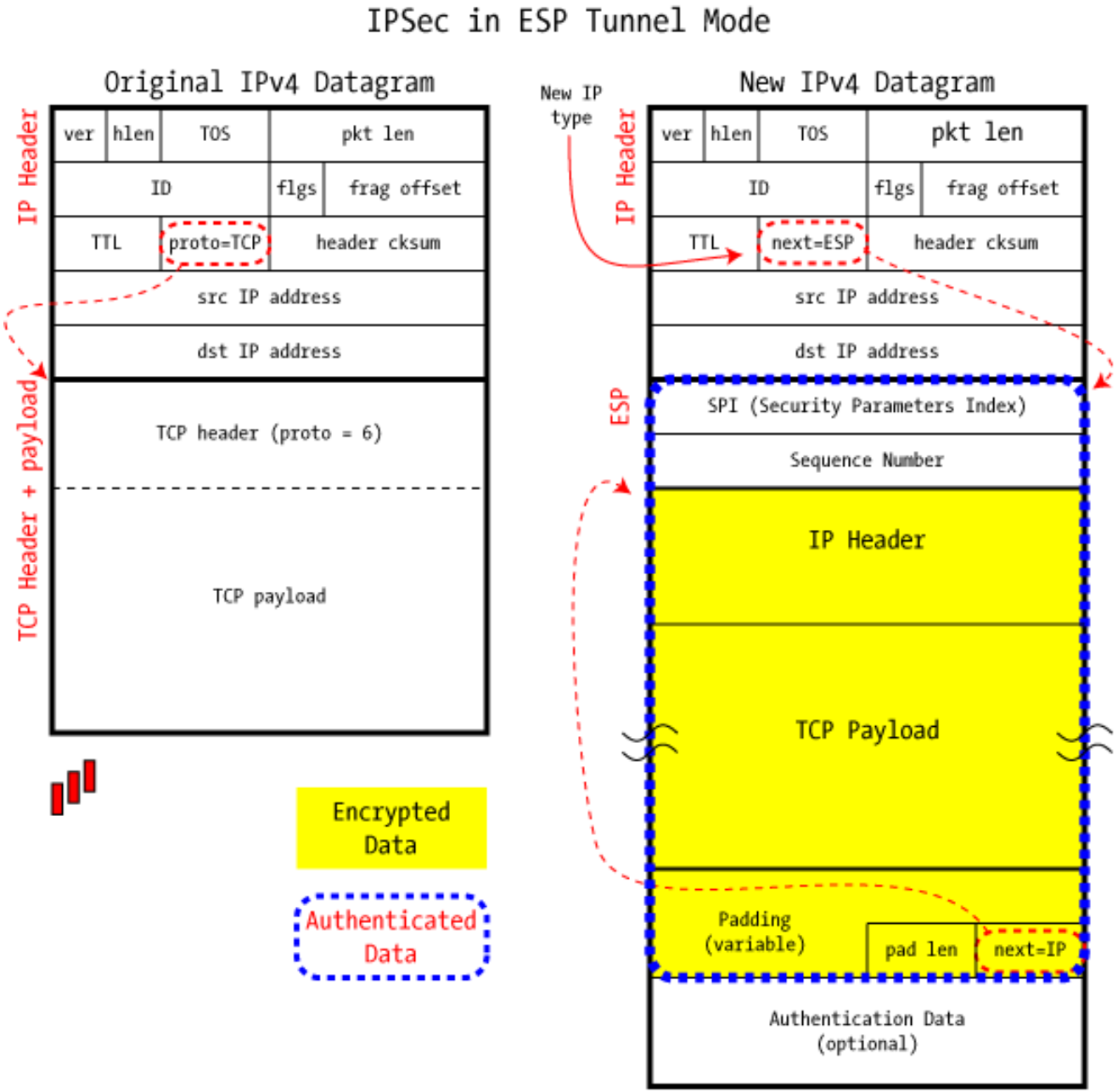
IPsec HMAC (AH auth)



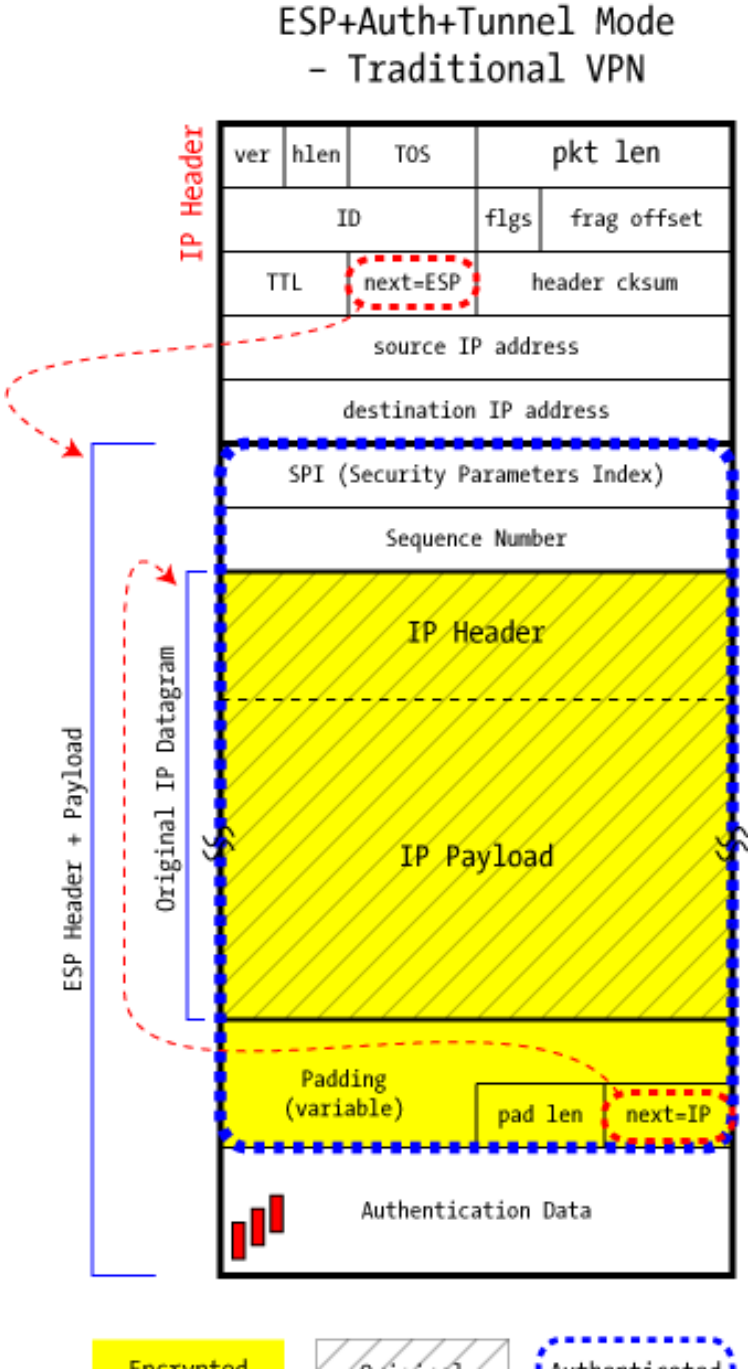
IPsec ESP/Transport mode



IPsec ESP/Tunnel mode



IPsec a final use



Q and A

- Thanks for listening.
- http://www.csrrt.org.lu/
- adulau@foo.be