Advanced Network Security

IPsec

Thomas Martin

t.martin@mmu.ac.uk

March 6, 2019

Outline

Introduction

IPsec is a suite of protocols for authenticating and encrypting IP packets[1]. It can establish mutual authentication between communicating devices and negotiate keys to be used in the session.
IPsec is an end-to-end scheme, meaning that it operates between the end-point sender and receiver (and not between routing intermediaries). It operates in the Internet Layer of the TCP/IP model. The main advantage of this is that it can immediately protect any application traffic on an IP network (whereas HTTP requires modification to use SSL/TLS). The downside is that it is quite technically complex, both in description as well as implementation.

[1] http://www.unixwiz.net/techtips/iguide-ipsec.html

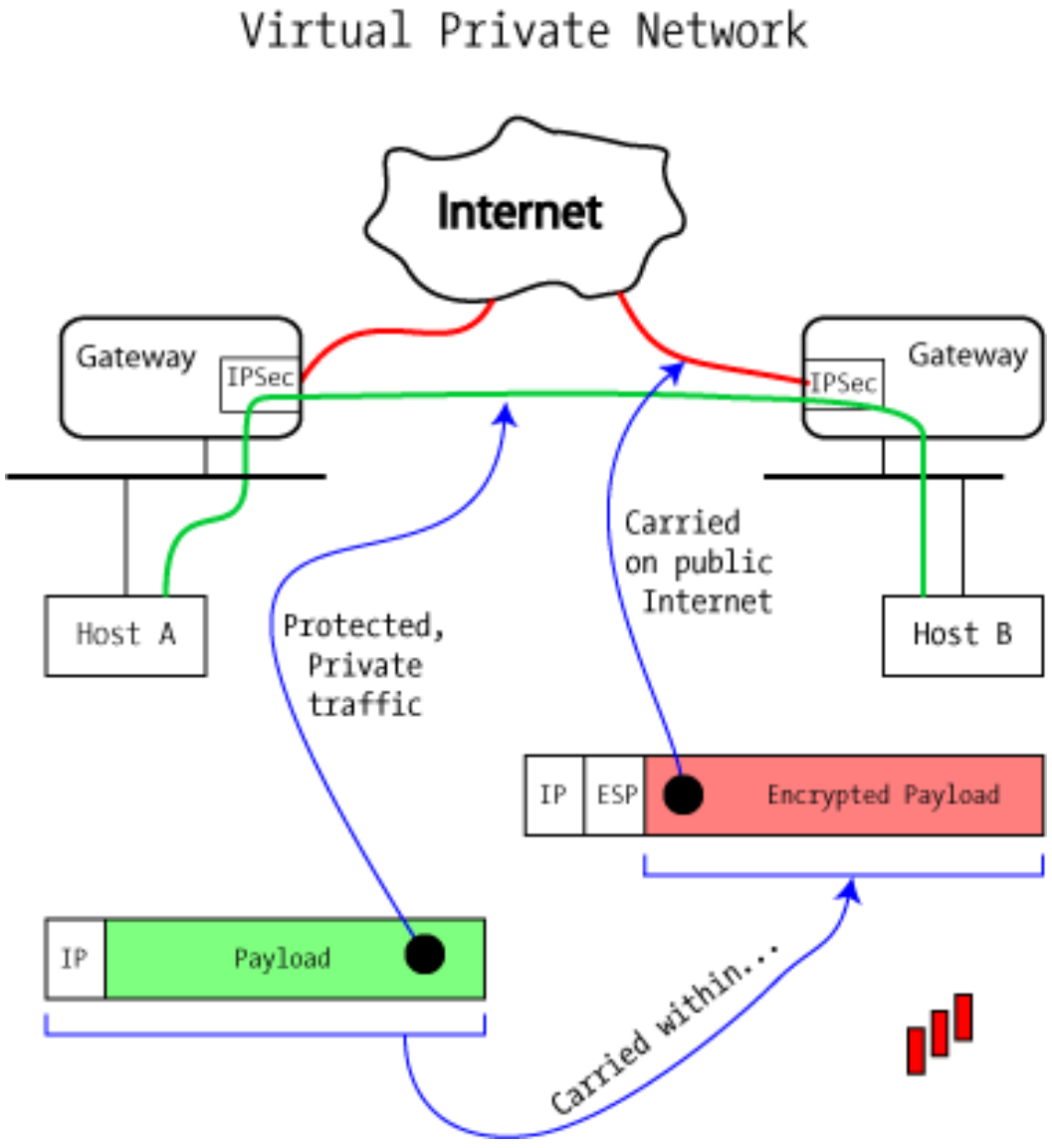
IPsec Protocols

The two main protocols of IPsec are **Authentication Header** (AH) and **Encapsulating Security Payload** (ESP). AH is concerned only with ensuring the integrity of the data (as well as the identity of the sender), whereas ESP provides confidentiality as well.

IPsec can be used in **Transport** or **Tunnel** mode. Transport mode encapsulates the payload, while Tunnel mode provides extra protection by encapsulating the entire packet.

Like the cipher suites in SSL/TLS, IPsec allows for the use of several different cryptographic algorithms. For authentication, an Integrity Check Value (ICV) is produced from any of a number of (keyed) hash functions. Encryption can be performed using the common algorithms, e.g. DES, 3DES, Blowfish, AES.

IPsec VPN (Tunnel Mode)

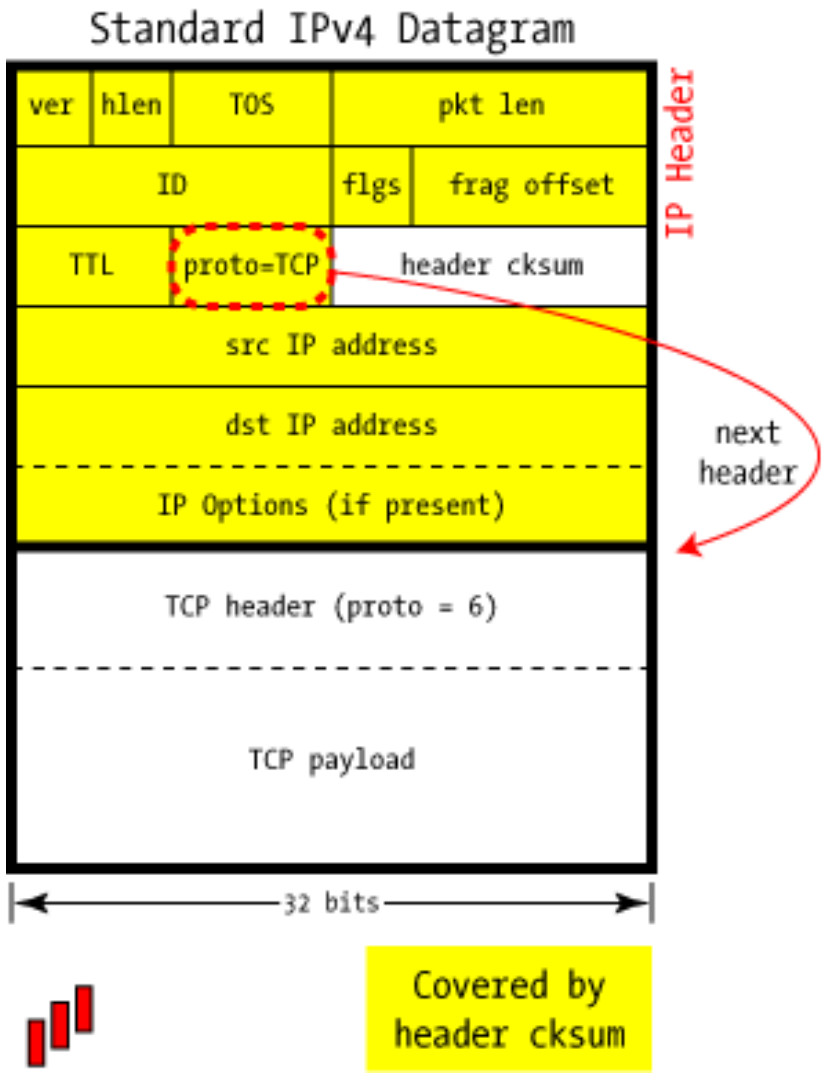


Key Agreement

Keys can be provided to both hosts manually, or through one of the means provided in the Internet Security Association and Key Management Protocol (ISAKMP). These include:

- Internet Key Exchange (IKE) - uses X.509 certificates and a Diffie-Hellman key exchange to setup a shared session secret.
- Kerberized Internet Negotiation of Keys (KINK) - peers authenticate with their Authentication Server using the Kerberos Protocol, with the KDC distributing the secret keys.
- IPSECKEY DNS records - contains public keys that can be used in key agreement.

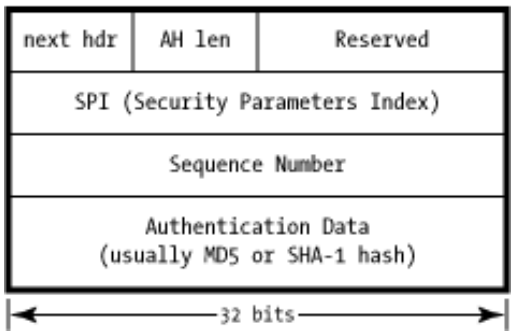
IP Datagram


Standard IPv4 Datagram
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
IP Options (if present)
IP Header
next header
TCP header (proto = 6)
TCP payload
32 bits
Covered by header cksum

AH: Authentication Only

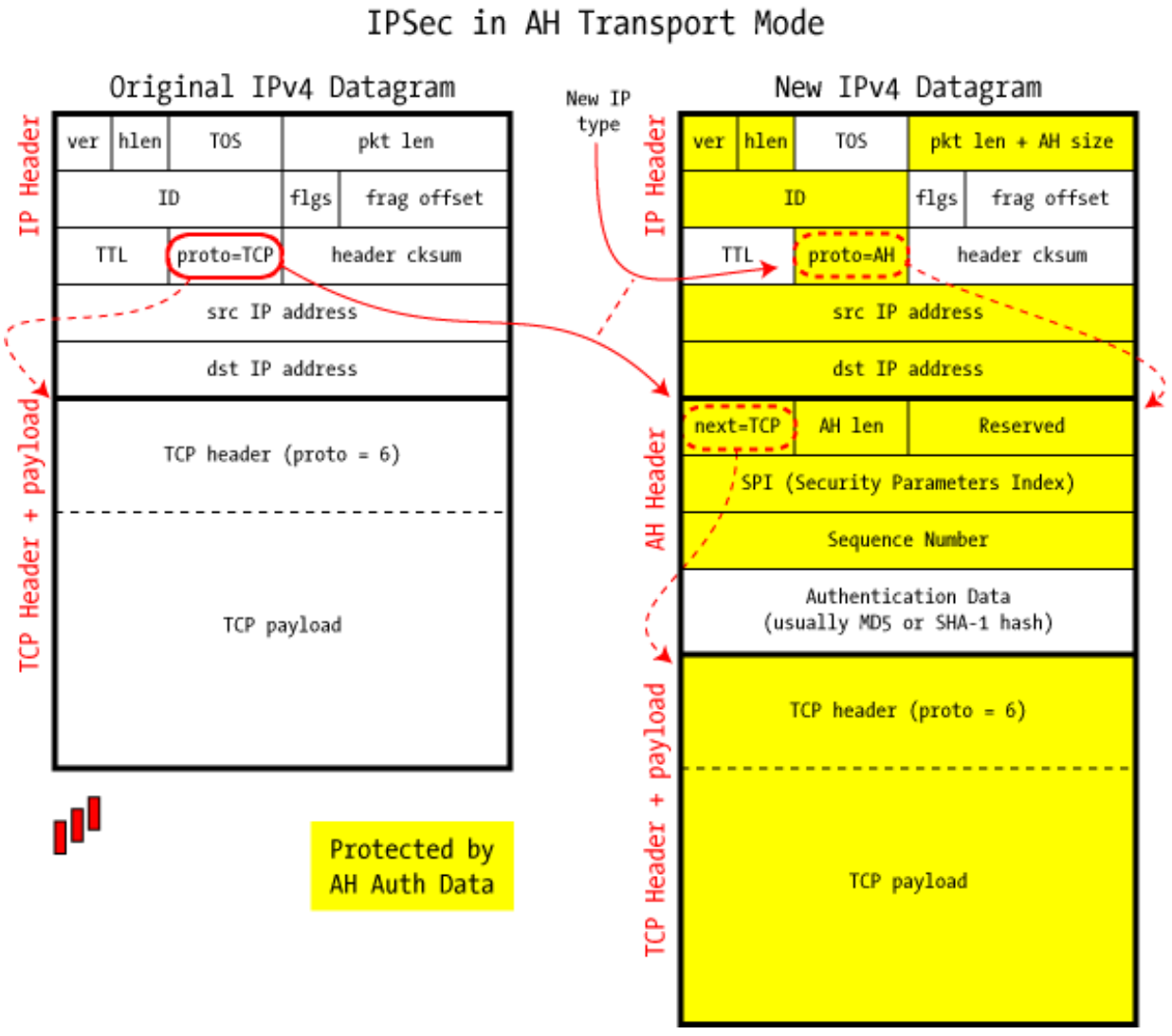
The purpose of AH is to ensure both parties are communicating with who they think they are, that data altered in transit will be identified, and that old data re-injected into the channel will be detected. A hash is calculated of the IP packet, but not of the entire packet. Some values, such as TTL, have to change, so these are omitted from the hash.

IPSec AH Header



The important fields of the header are:
next hdr: identifies the protocol type of the following payload
AH len: length of the whole AH header
Security Parameters Index: Index for the type of cryptographic operations used in creating the packet
Authentication Data: ICV calculated over almost all of the packet

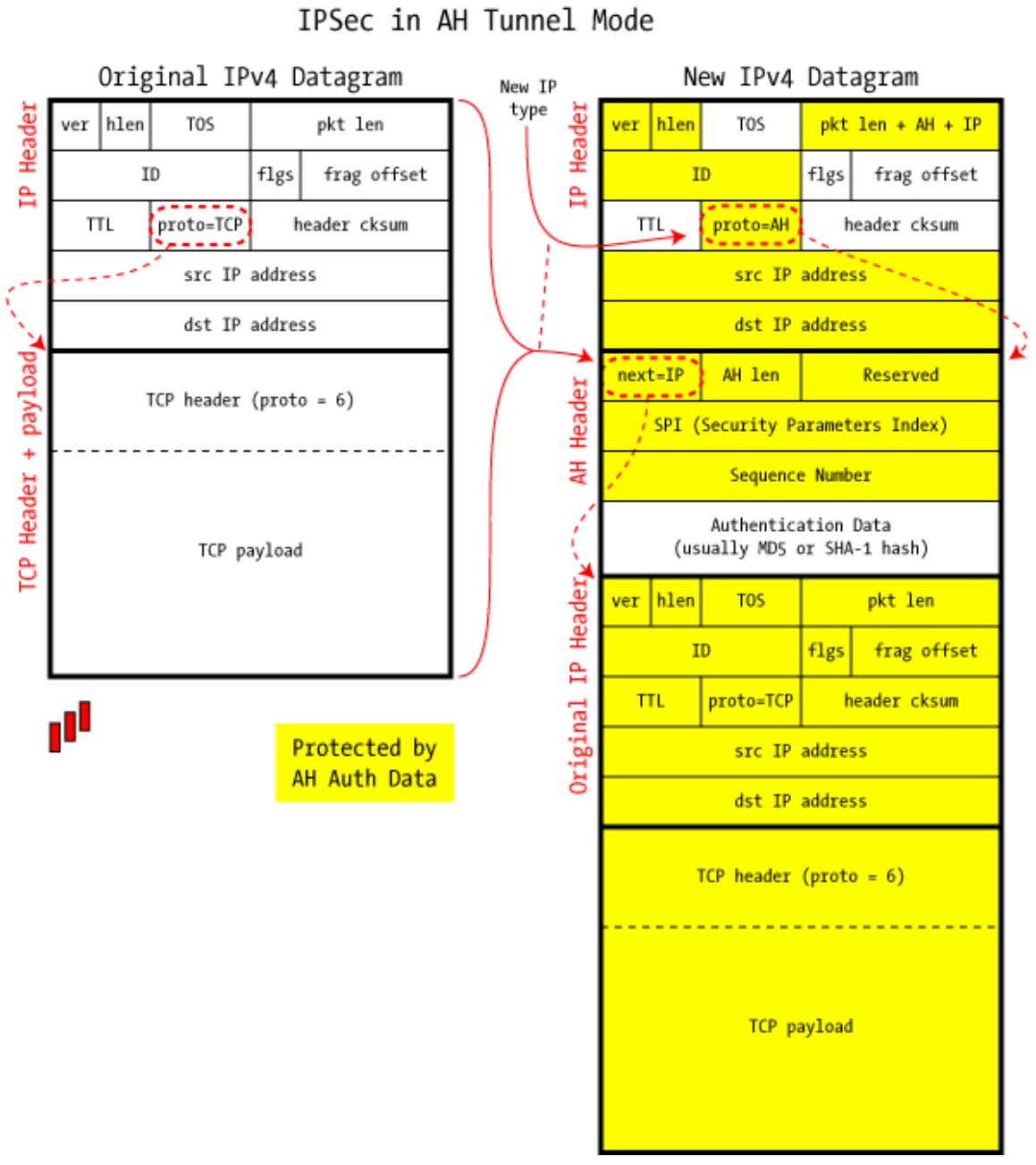
AH Transport Mode



Transport Mode is used to protect an end-to-end conversation between two hosts. The new AH header is placed between the IP header and the protocol payload. The original protocol type is removed and replaced with one identifying it as AH. Once the receiving host has verified the correctness of the cryptographic hash, the header is stripped and the original protocol type restored.

With Tunnel Mode, the entire original IP packet is encapsulated inside another. There are two separate IP headers (which can have different source and destination addresses). When the packet arrives at its destination, it goes through the same checks as with Transport mode. If it passes, the original IP datagram is reconstructed. This packet can be delivered to the local machine, or sent elsewhere. While Transport Mode must be used end-to-end, Tunnel Mode can be used between gateways to provide a Virtual Private Network (VPN).

AH Tunnel Mode



Authentication Header and NAT

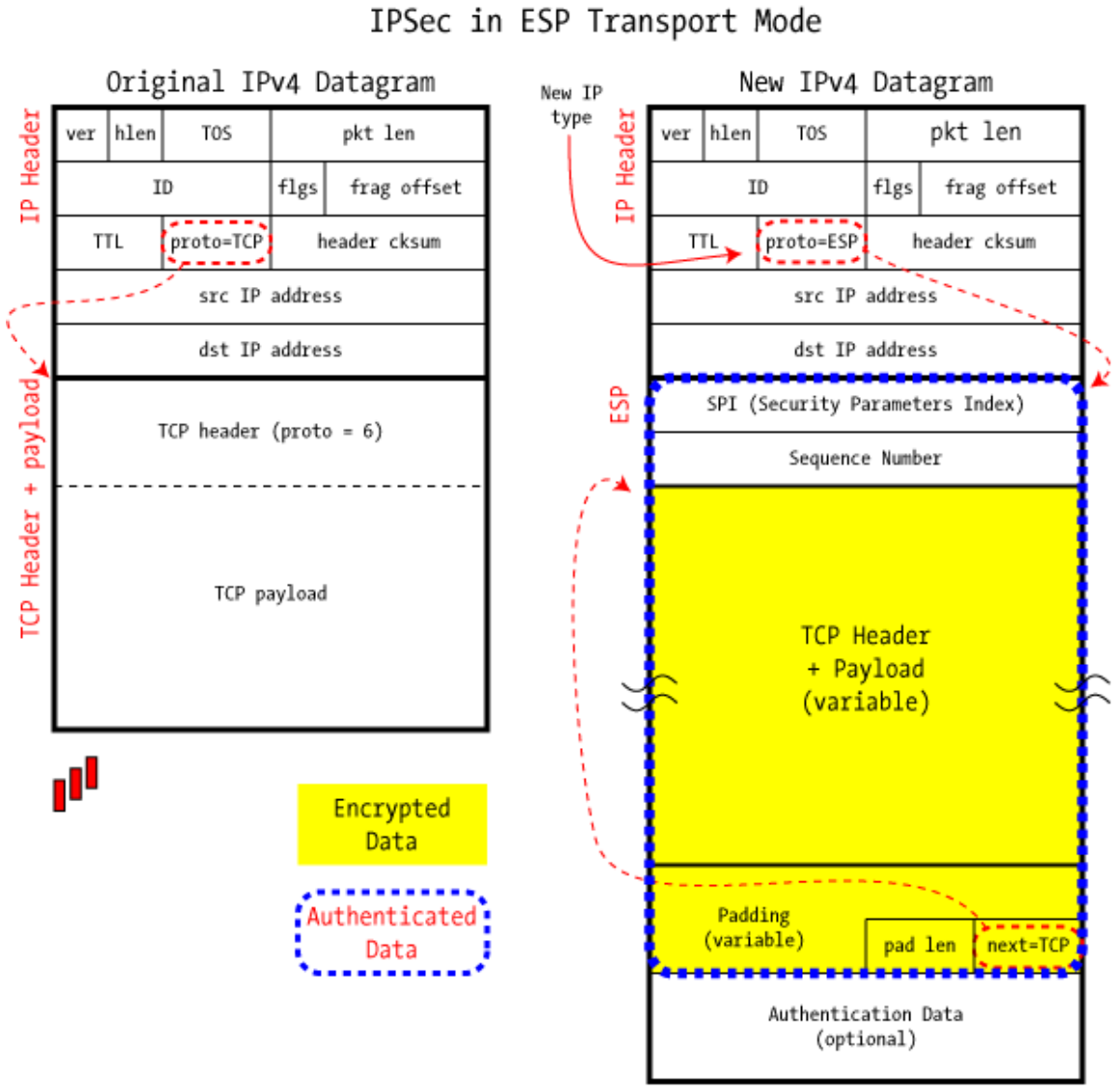
The use of Transport or Tunnel Mode is not explicitly identified. If the next-header value is IP, it means an entire IP datagram is being encapsulated. This is Tunnel Mode. Any other value indicated Transport Mode.

Network Address Translation (NAT) maps a range of private addresses to a single (or small set of) public address(es). This requires that the IP header be modified by the router. These changes make it incompatible with AH. Because both IP addresses are included, when the router changes them, the ICV is no longer correct, and will be rejected by the destination. The TTL field and header checksum are also changed by all network devices forwarding packets, but these are not included in the ICV.

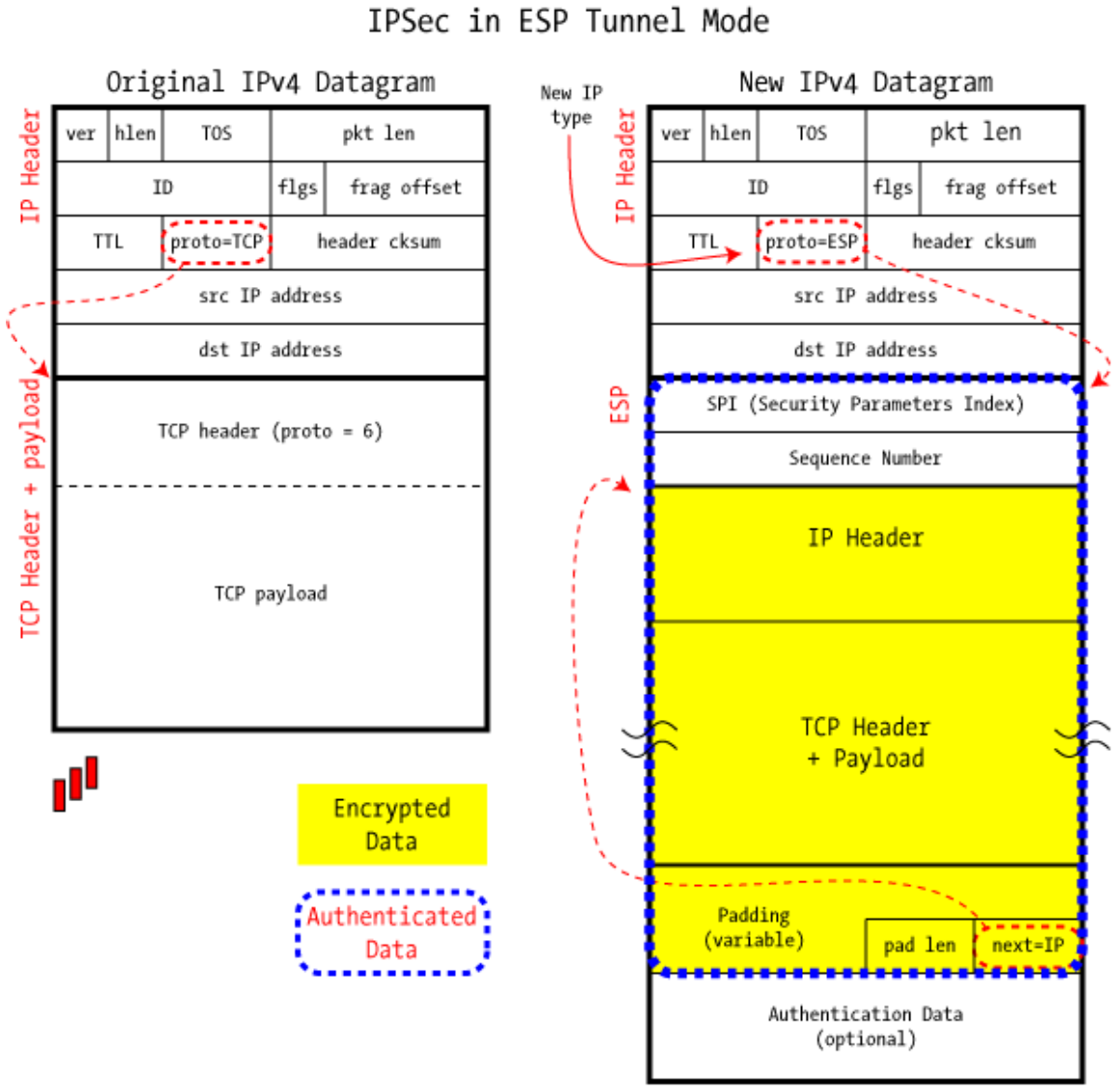
Encapsulating Security Payload

Whereas AH provides a small header before the payload, ESP encrypts and replaces the data it is protecting. The SPI and sequence numbers are present as before, but padding length and next header at the end. Optionally, authentication of the data can be added as with AH, but this is only for the ESP header and encrypted payload. ESP leaks very little information. The source and destination IP addresses are visible, as is the fact that it is an ESP packet, but even the packet type is encrypted.
Like AH, ESP can be used in Transport or Tunnel Model. However, unlike AH, this flag is encrypted, so is only known to the end-points.

ESP Transport Mode



ESP Tunnel Mode



Security Associations

When IPsec packets arrive at a host, it needs to know how to process it (what keys/algorithms to use). With each channel there is a corresponding **Security Association** (SA). These are stored in a Security Associations Database (SADB), and are indexed using the partner IP address, IPsec protocol (ESP/AH) and SPI. Security associations are one way, meaning two are required for ESP between two hosts. Within the SADB is stored:

- AH: authentication algorithm and secret
- ESP: encryption algorithm and secret key (and if authentication is enabled)
- Key exchange parameters
- Routing restrictions
- IP filtering policy

IPsec VPN

The aim of a VPN is to join two networks over an untrusted intermediate network, with the security equivalent to what you would get if you used a very long Ethernet cable. Using ESP with Authentication in Tunnel mode is typically used to achieve this. ESP can be used with AH, but that has the limitation of not being compatible with NAT. The authentication in ESP does not include the IP addresses. A benefit of this approach is transparency, and zero configuration, on the part of the end users. All the work is done by the gateways, and yet the users get the benefits of confidentiality and integrity of all traffic (for all applications) between the trusted networks.

Thank you

Relevant chapter:
Kaufman, Network Security, Chapter 17.

Any Questions?