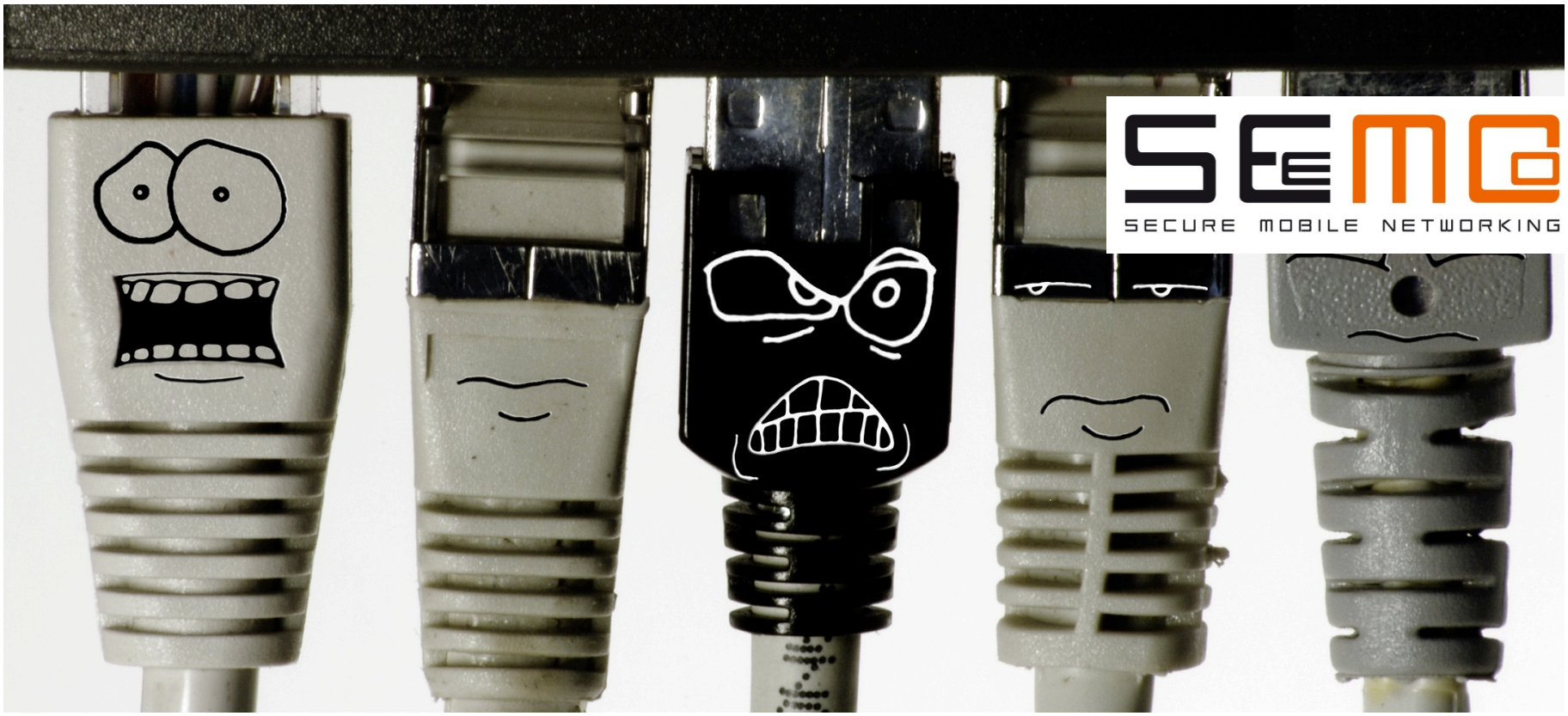
Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 05: Network Level Security
Module 02: IP Security (IPSec)



SECURE MOBILE NETWORKING

CASED

Learning Objectives

How network level security can be implemented in a comprehensive fashion

Understand IPSec…

- …architecture
- …modes of operation
- …features
- …trade-offs

Overview of this Module

(1) IPSec Introduction
- Building Blocks

(2) Protection mechanisms
- Authentication Header (AH)
- Encapsulated Security Payload (ESP)

(3) Modes of Operation
- Transport Mode
- Tunnel Mode

We discuss these aspects with increasing level of detail

Chapter 05, Module 02

Recap: Security Problems of the Internet Protocol (IP)

When an entity receives an IP packet, it has **no** assurance of:

1. Data origin authentication/data integrity:
   - The packet has actually been send by the entity which is referenced by the source address of the packet
   - The packet contains the original content the sender placed into it, so that it has not been modified during transport
   - The receiving entity is in fact the entity to which the sender wanted to send the packet

2. Confidentiality:
   - The original data was not inspected by a third party while the packet was sent from the sender to the receiver

IPSec…

…offers security on network layer

- Need for authentication and encryption in IPv4 & IPv6 identified in 1994 report "Security in the Internet Architecture" (RFC 1636)

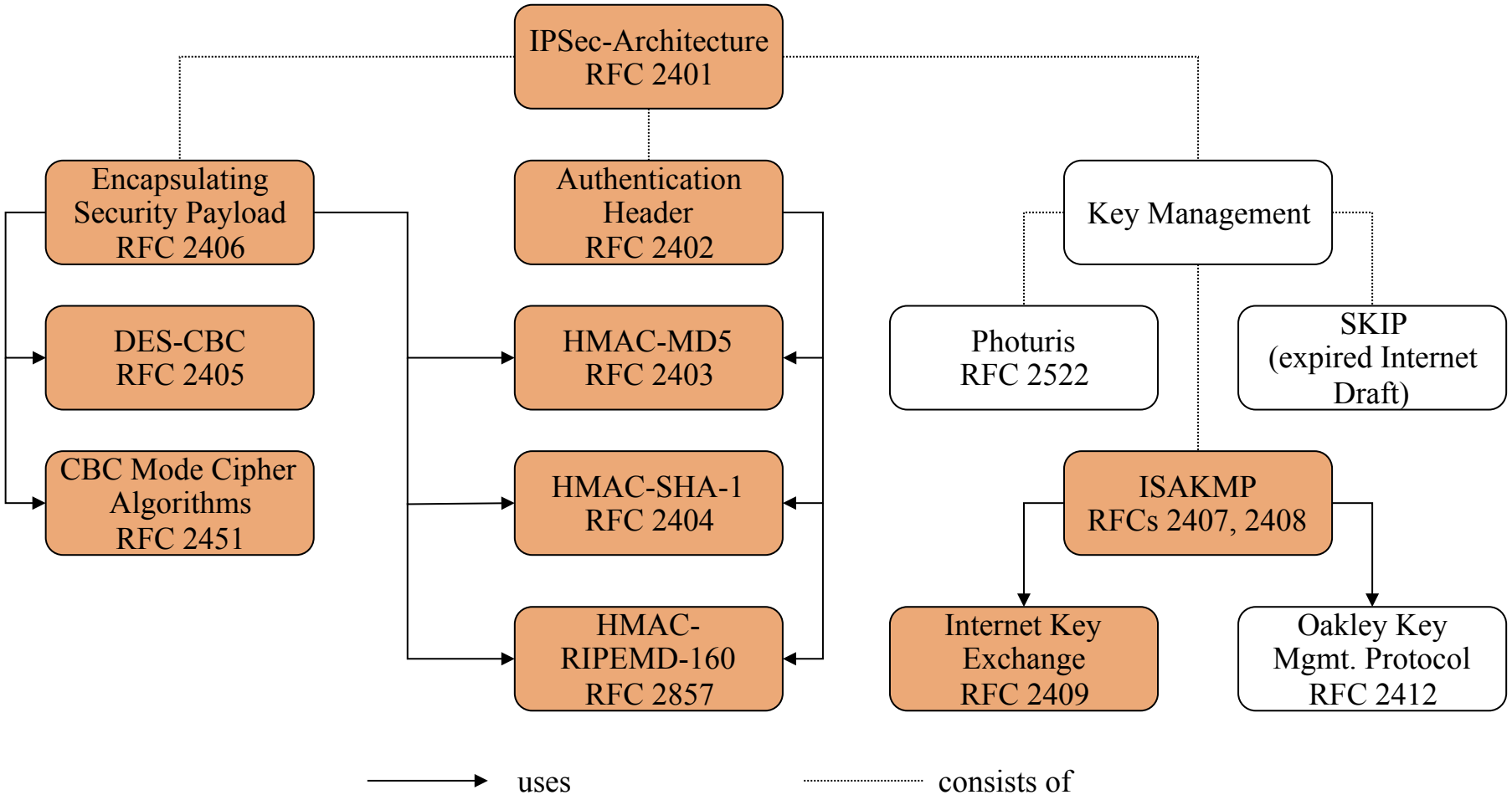
…was first standardized by IETF in 1998

- RFC 2401 - Main Document (now obsolete ➔ RFC 4301)
- RFC 2402 - Authentication Header (AH) ➔ RFC 4302
- RFC 2406 - Encapsulating Security Payload (ESP) ➔ RFC 4302
- Securing the data is based on symmetric encryption (for performance reasons)

- History bits and an excellent treatment of the topic can be obtained by reading the book of Perlman, Kaufman et al. (who have been part of the IETF IPSec WG)


Kerkkaars
Nr. 202080
12 Stuks
KSD
ITEM# 202080
Rotterdam
Order No. 23597
C/NO.: 110 – 225
wooden deco cake stand 2-layer
Nr 533445
KSD
ITEM#533445
Rotterdam
order no.: 29078
C/NO:

Overview of the IPSec Standardization (History)



IP Security Architecture

Original IPSec RFCs have been overhauled in 200x

IPSec specification is quite complex, can be clustered in:

- Architecture
  - RFC4301 Security Architecture for Internet Protocol
- Authentication Header (AH)
  - RFC4302 IP Authentication Header
- Encapsulating Security Payload (ESP)
  - RFC4303 IP Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)
  - RFC4306 Internet Key Exchange (IKEv2) Protocol

- Cryptographic algorithms
- Other (check out http://datatracker.ietf.org/wg/ipsec/charter/)

IPSec - Overview

IPSec is based on the paradigm of a „connection”

- …despite the fact that IP is connectionless

Connection is called "Security Association (SA)“

Connection paradigm is necessary to protect certain assets

Provides security services

- Connectionless integrity
- Data origin authentication
- Confidentiality (encryption)

- Rejection of replayed packets
  - a form of partial sequence integrity

- Limited traffic flow confidentiality
- Access control

IPSec - Overview

IPSec introduces protection protocols

- extra header between layer 3 and 4 (IP and TCP) to give the destination enough information to identify the „security association”
- Authentication Header (AH)
  - Offers message integrity and source authentication but **not** message confidentiality
- Encapsulating Security Payload (ESP)
  - Offers source authentication, message integrity and confidentiality

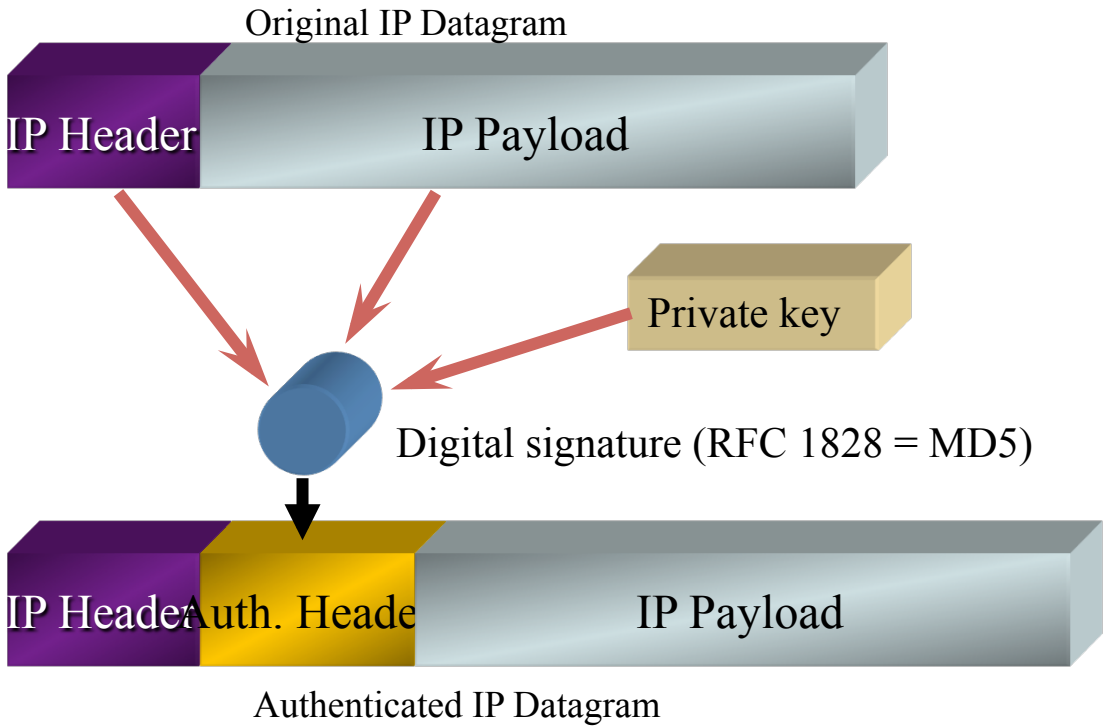
Can be run in two modes

- Transport mode for host-based end-to-end security
- Tunnel mode for security between network borders

Authentication Header (AH)

IPSec Authentication Header (AH) contains an encrypted hash of the whole packet.

This allows the receiver to verify the authenticity of the addresses and the integrity of the payload and parts of the header



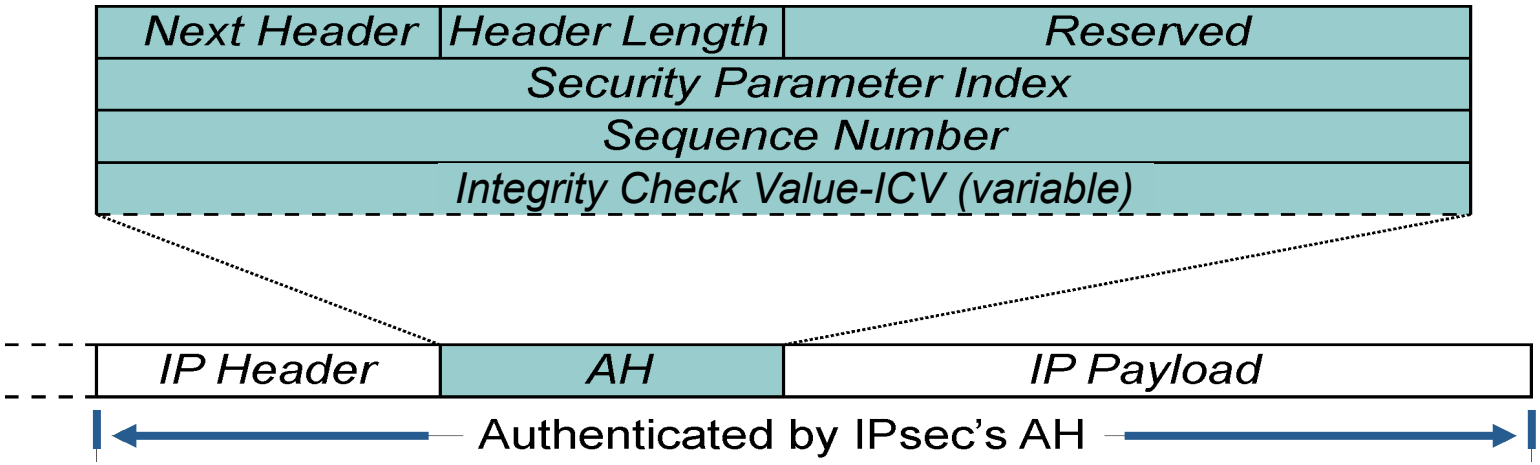
IPSec - Authentication Header (AH)

Authenticates

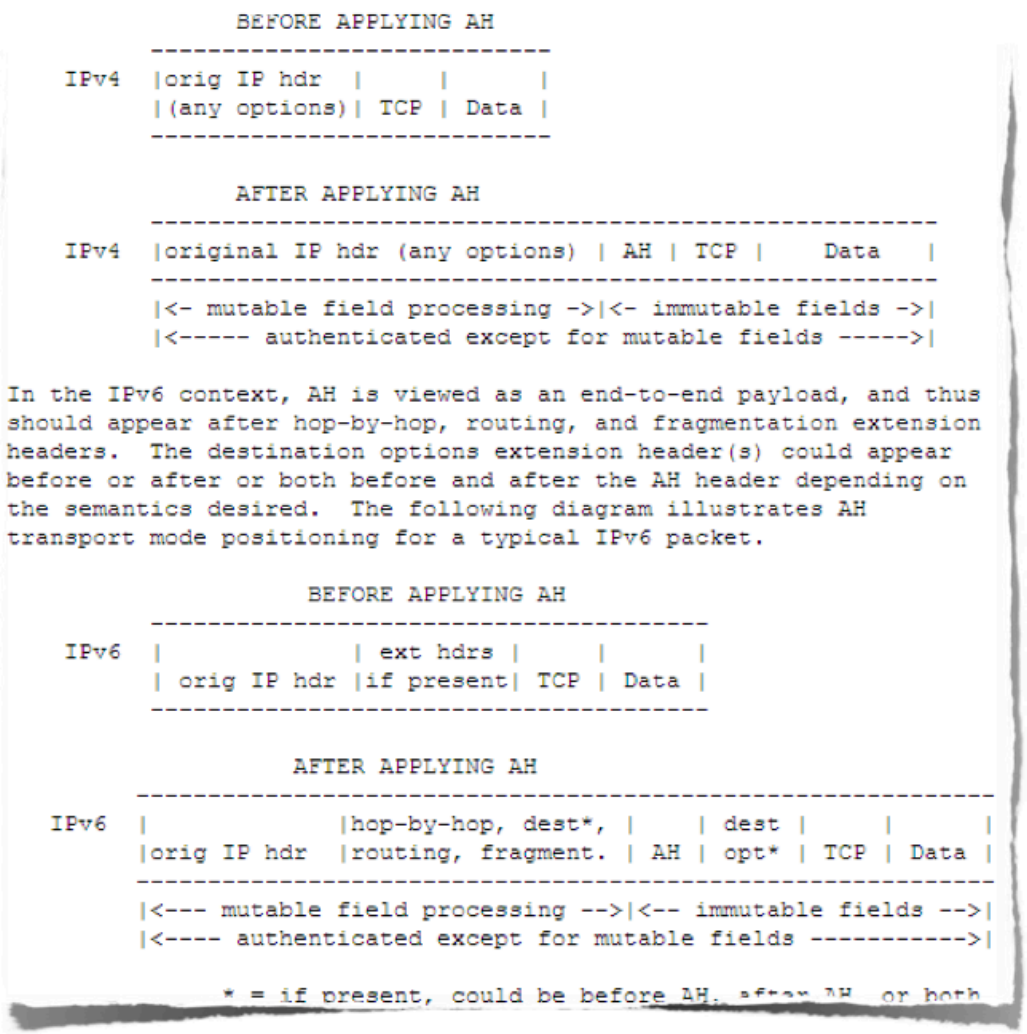
- IP Header (mutable fields are set to zero for computation)
- Itself (field "authentication data" is set to zero for computation)
- IP Payload (integrity protection)

Uses HMACs for authentication

- Specified are HMACs based on MD5 and SHA1

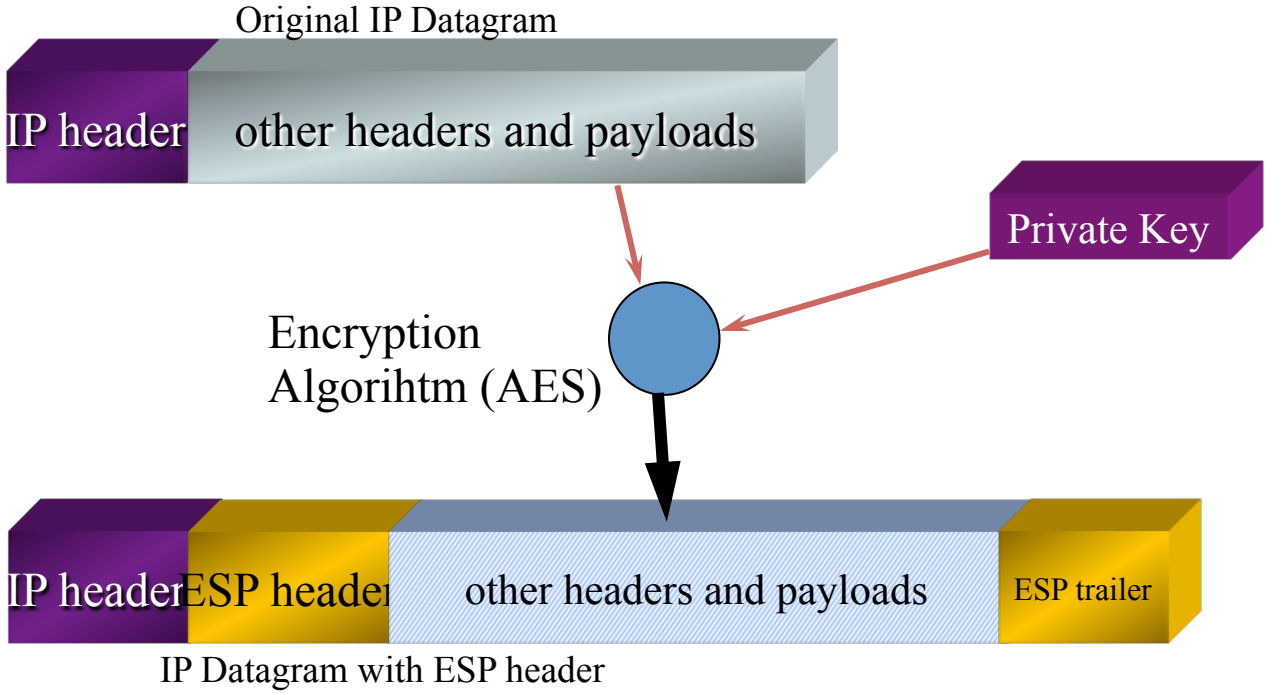


Protection of AH



Encapsulating Security Payload (ESP)

IPSec Encapsulating Security Payload (ESP) guarantees the integrity and/or confidentiality of the original datagram combining a secure hash and encrypting the IP payload or the whole IP packet



IPSec - Encapsulating Security Payload (ESP)

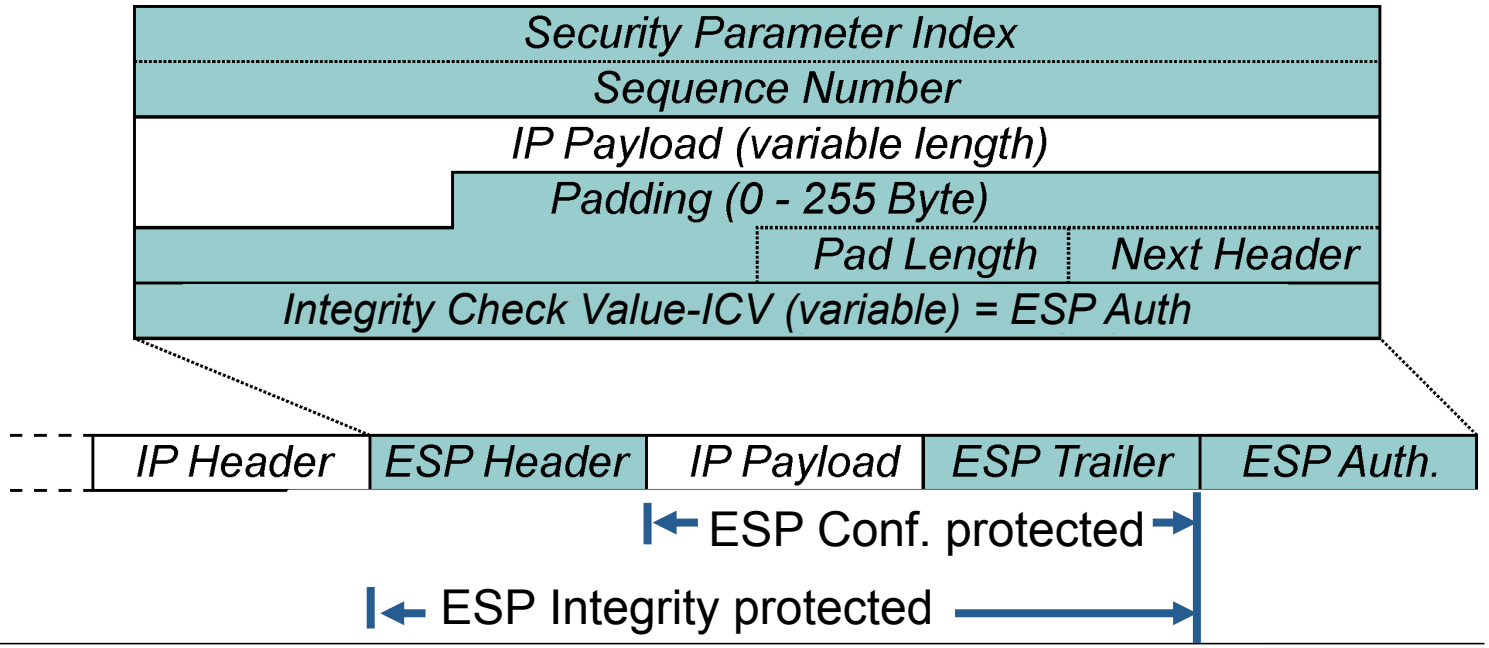
Authenticates itself, IP payload and ESP trailers

- HMACs, like with IPSec AH

Encrypts IP payload and ESP Trailer

- Symmetric encryption (DES, AES, …)

Can be combined with Authentication Header



Format of an ESP Packet

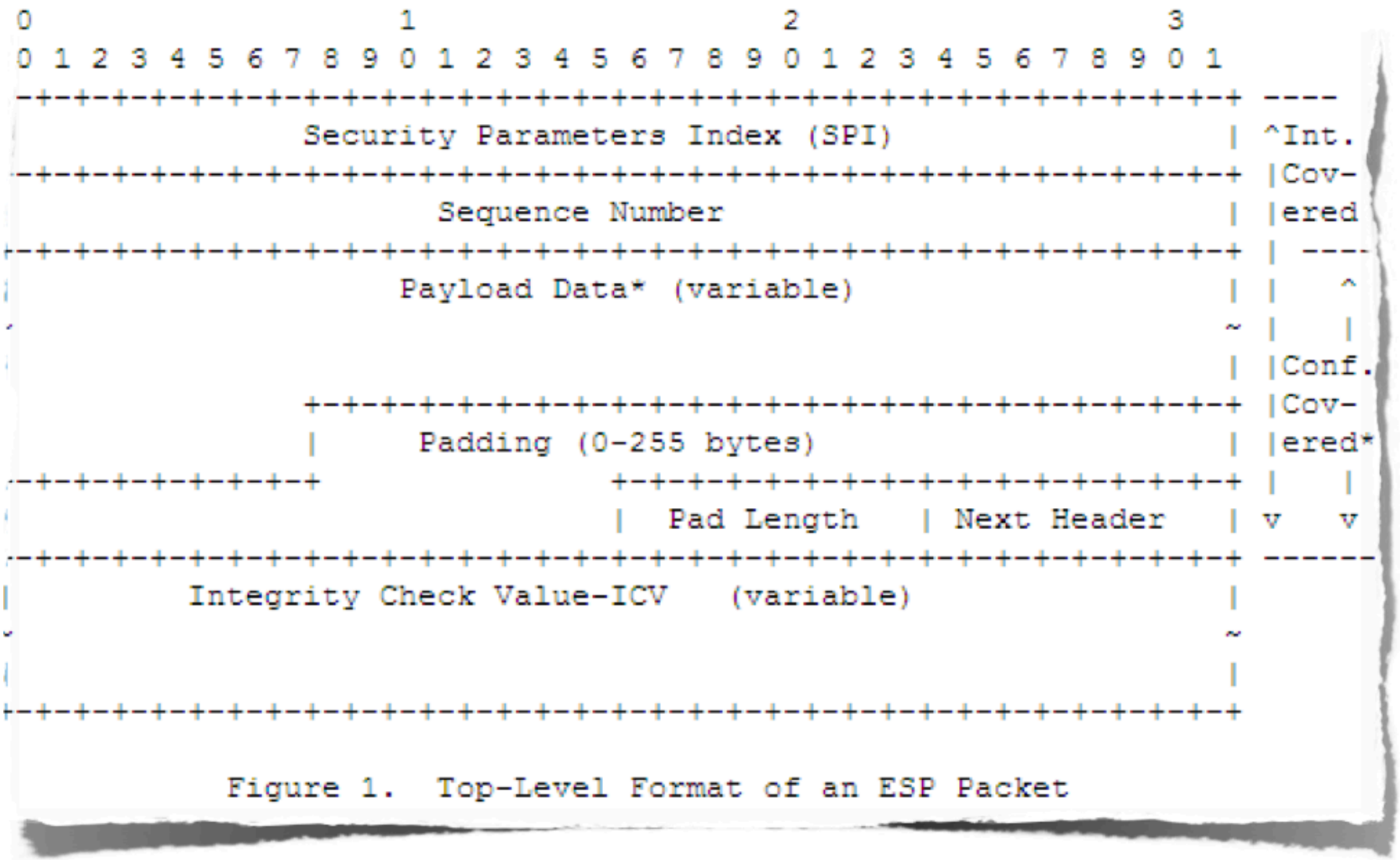
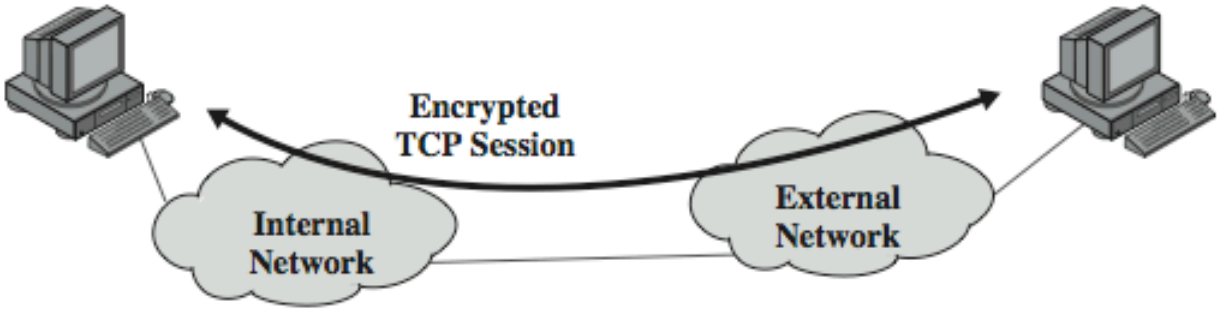


Figure 1. Top-Level Format of an ESP Packet

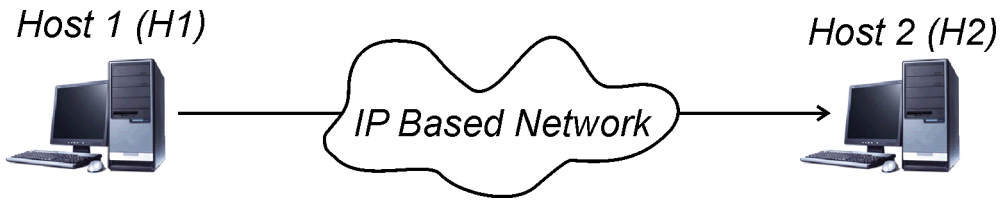
IPSec - Transport Mode



IPSec - Transport Mode

Sets up a secure end-to-end connection

- Between two hosts

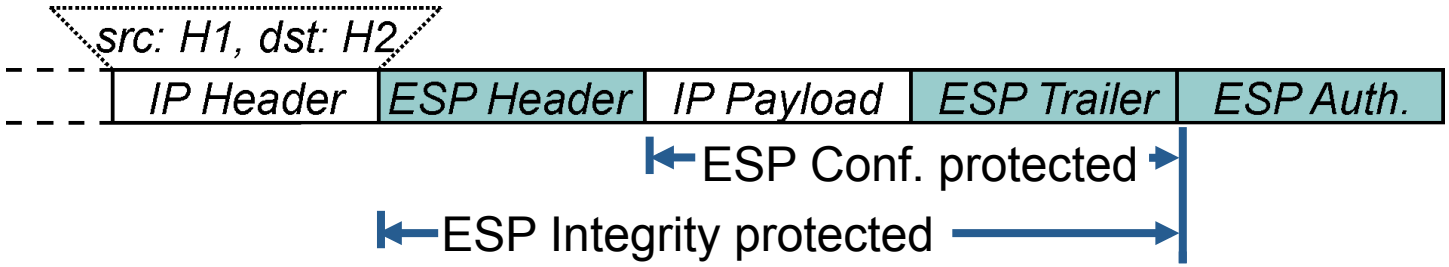


Keeps original IP header

- Protocol field is set to indicate that an IPSec header follows

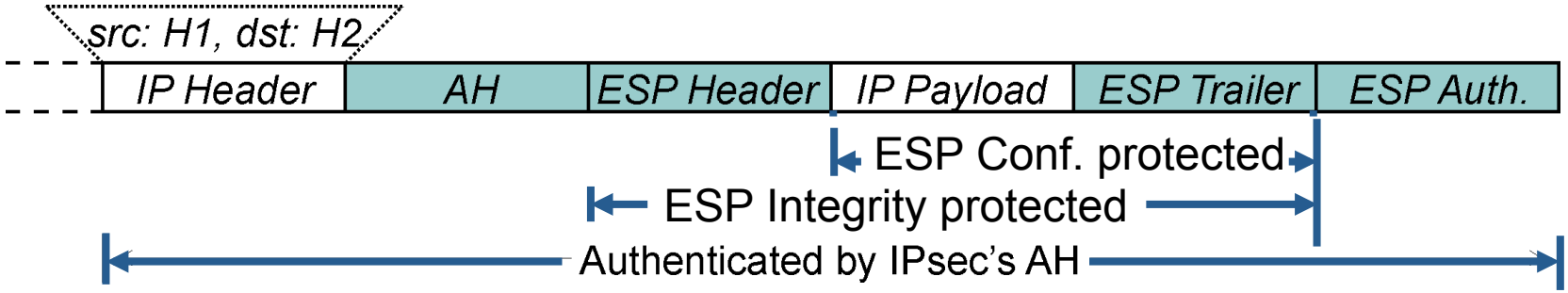
IPSec - Transport Mode

Can be used for Encapsulating Security Payload

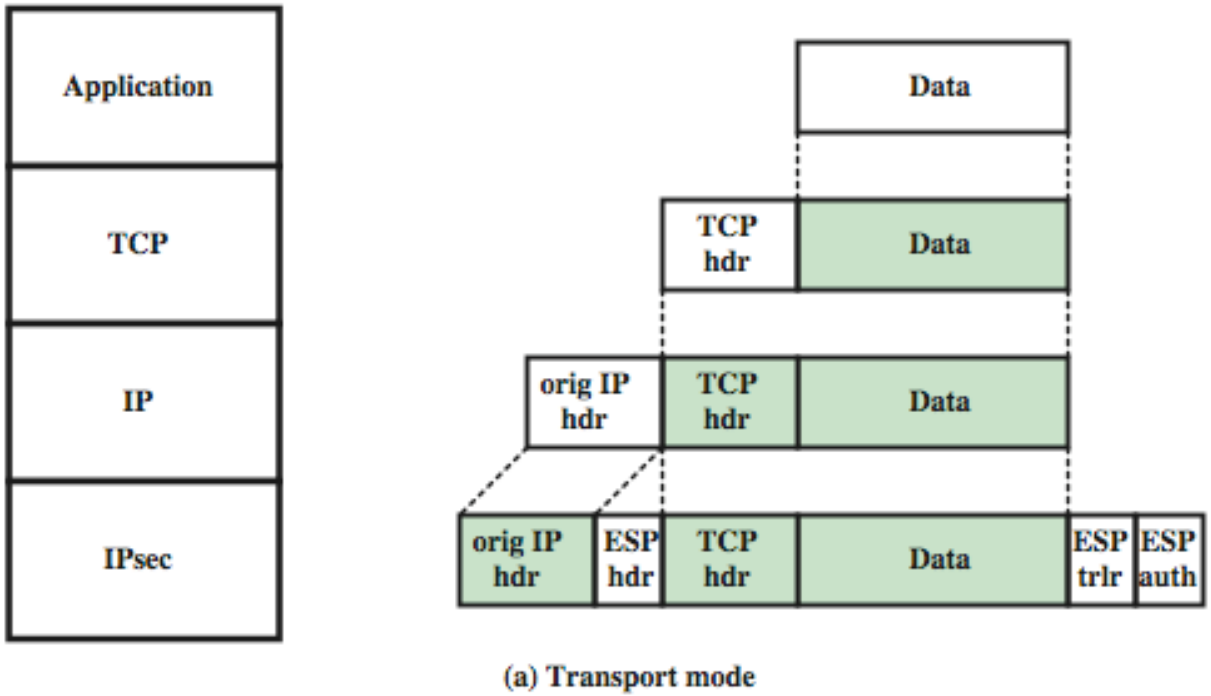


Can be used for AH & ESP

- To get encryption together with authenticated IP header

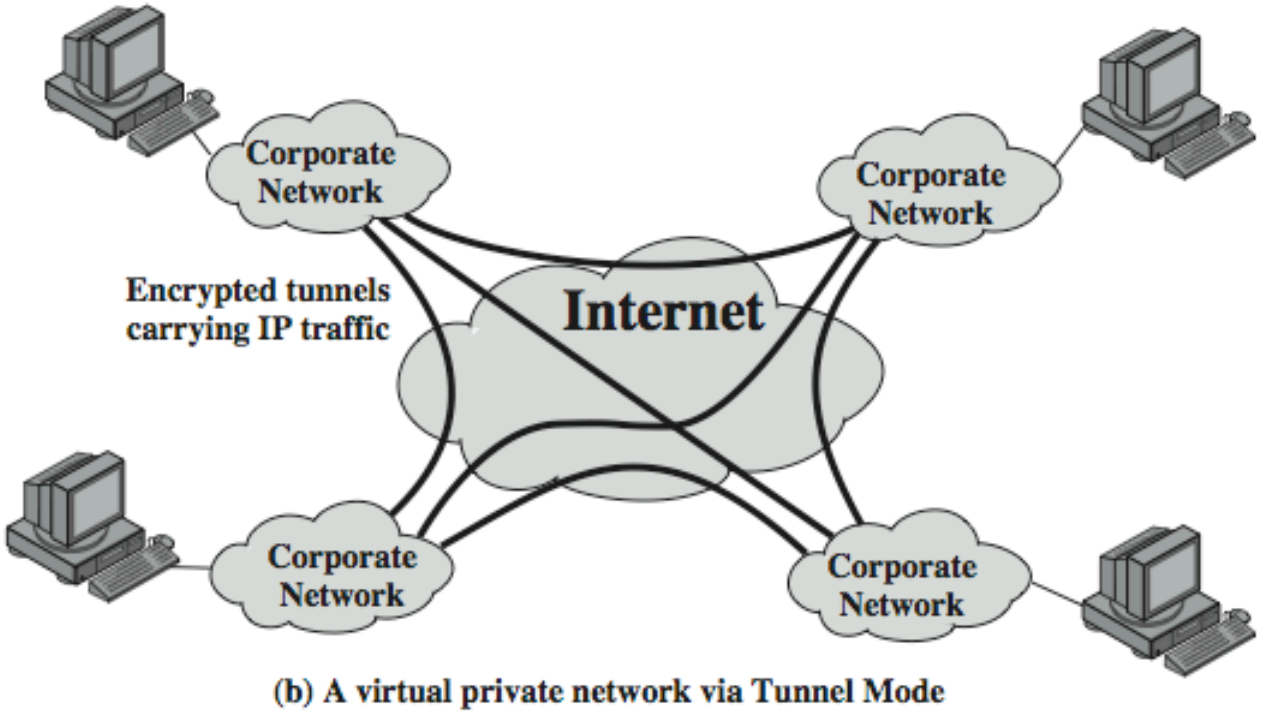


IPSec – ESP & Transport Mode



(a) Transport mode

IPSec - Tunnel Mode



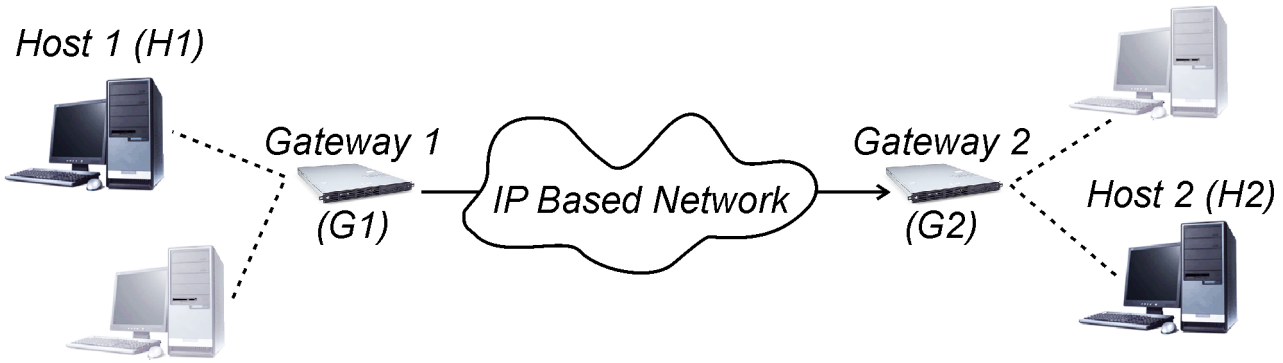
(b) A virtual private network via Tunnel Mode

IPSec - Tunnel Mode

Sets up a secure end-to-end connection

- Between two networks

→ Not every host has to be adapted / maintained

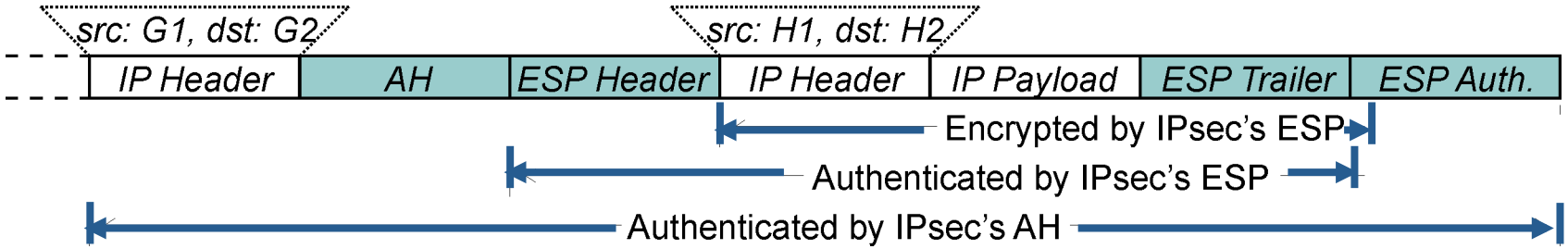


Introduces additional IP header

- With addresses of tunnel endpoints
- To prevent traffic analysis (when used with ESP)

IPSec - Tunnel Mode

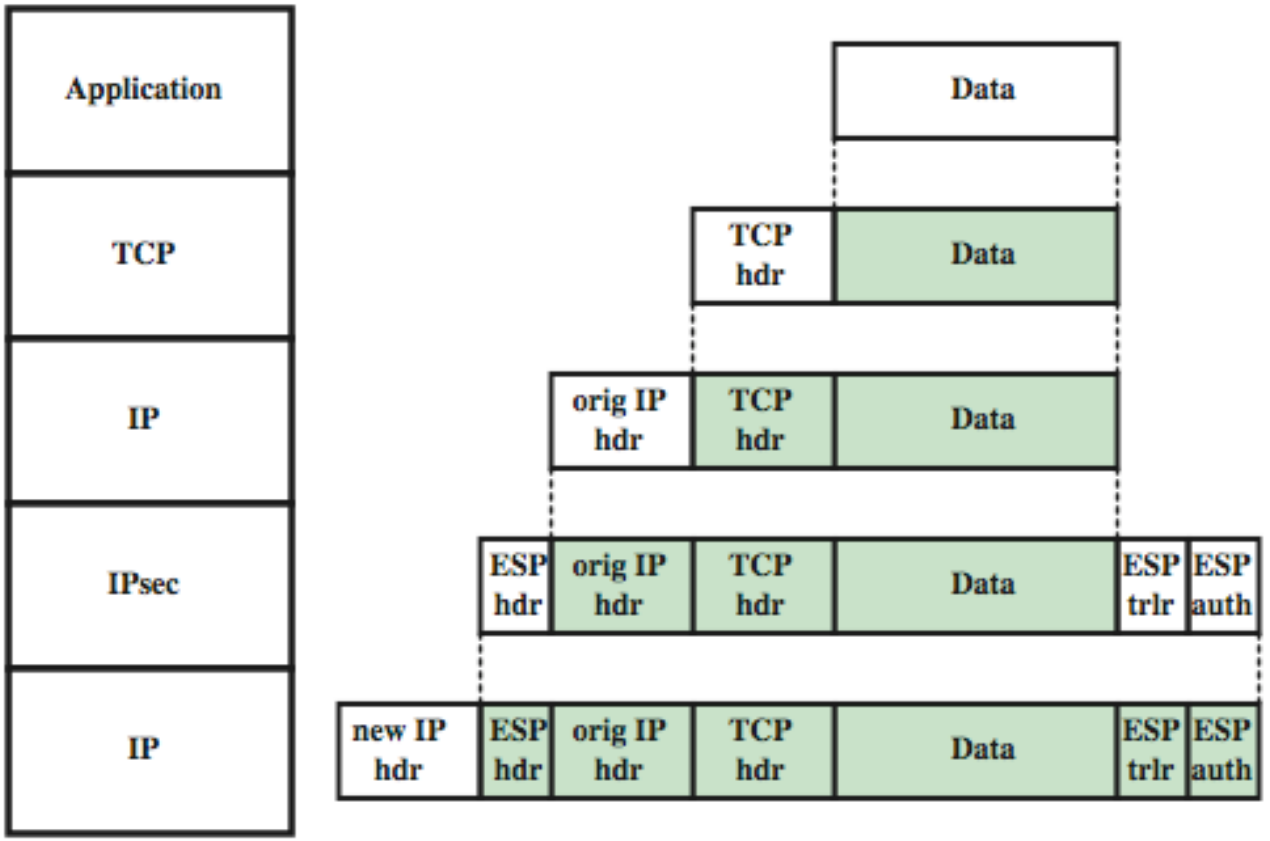
Can be used for AH, ESP, and both



Can be combined with transport mode

- Between hosts
- To obtain additional authentication / encryption

IPSec – ESP & Tunnel Mode



(b) Tunnel mode

Transport and Tunnel Mode

SECURE MOBILE NETWORKING

Transport Mode

- to encrypt & optionally authenticate IP data
- can do traffic analysis but is efficient (little overhead)
- good for ESP host to host traffic

Tunnel Mode

- encrypts entire IP packet
- add new header for next hop
- no routers on way can examine inner IP header
- good for VPNs, gateway to gateway security

Other pros and cons?

Transport and Tunnel Mode Pros and Cons

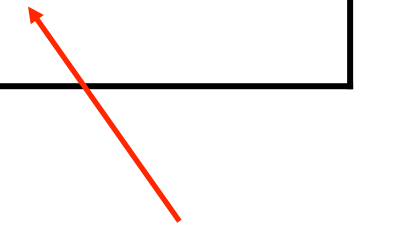
SECURE MOBILE NETWORKING

Transport Mode

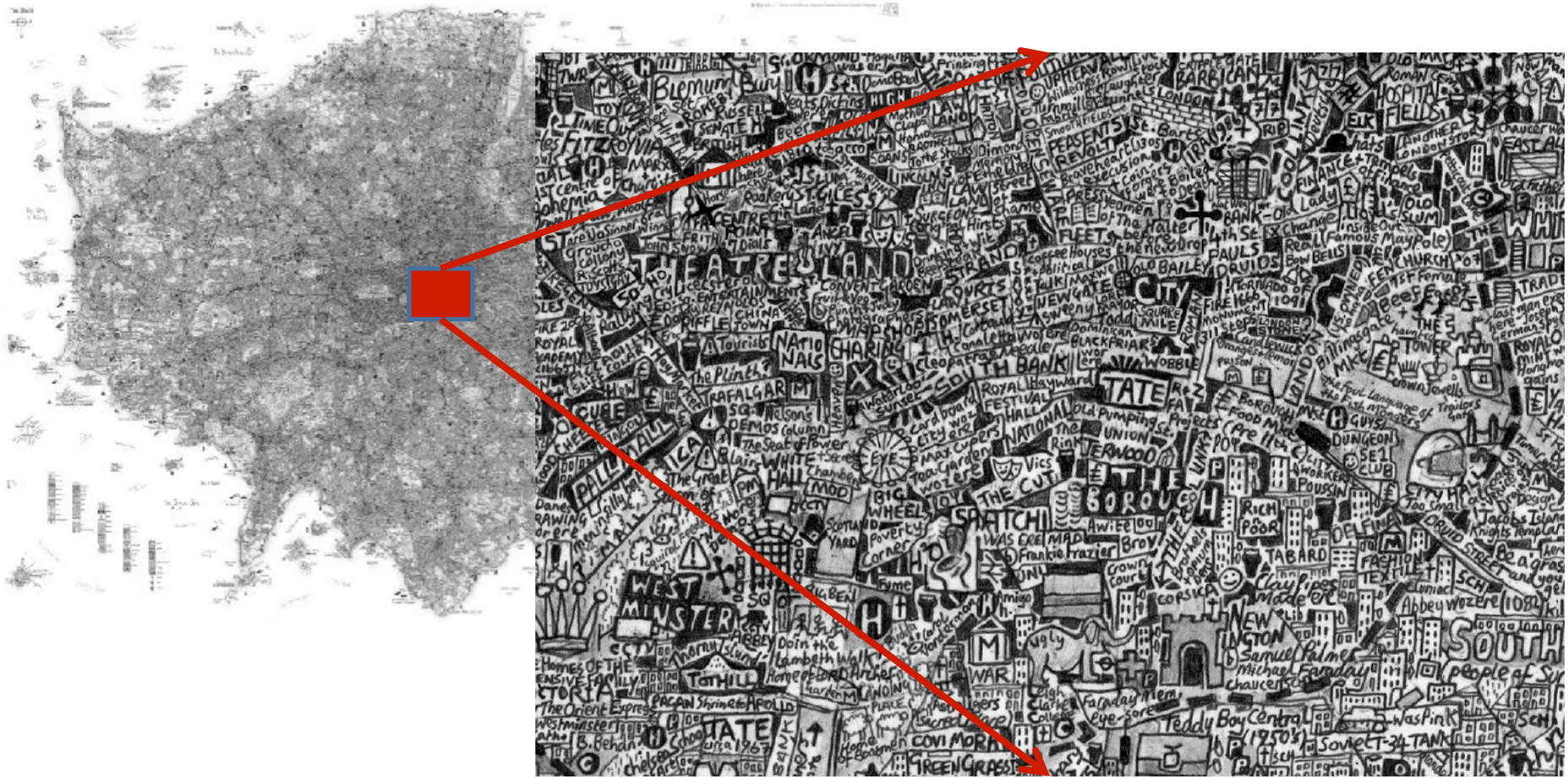
Tunnel Mode

Four combinations are possible

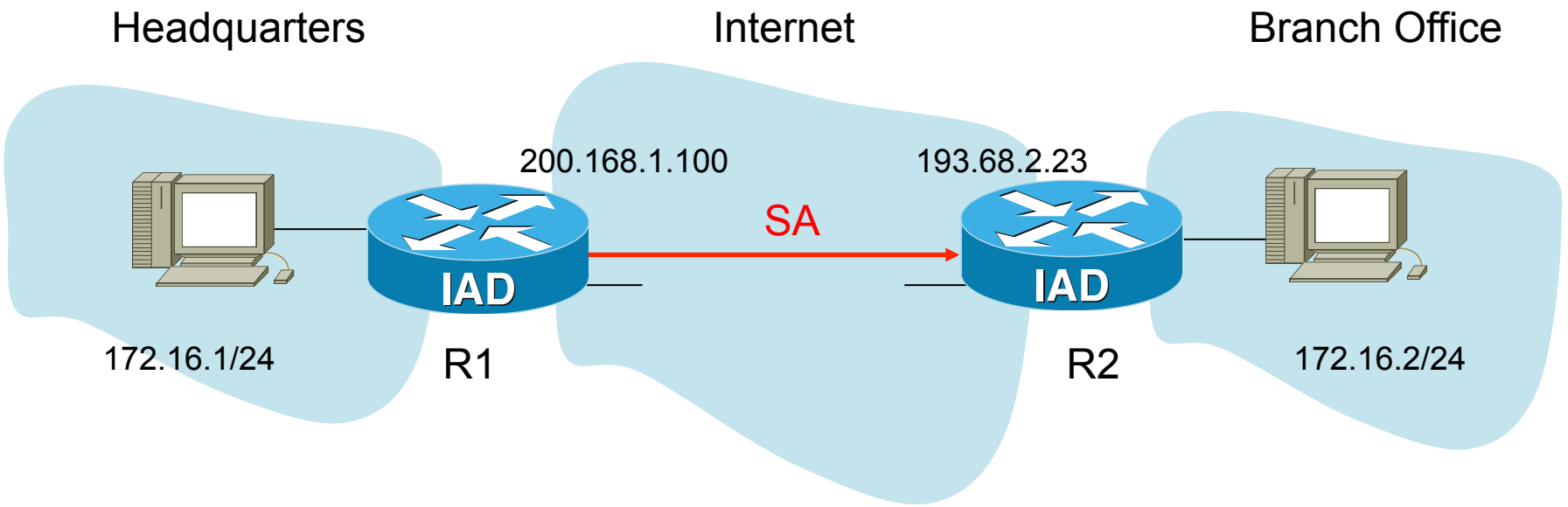
Transport mode with AH	Transport mode with ESP
Tunnel mode with AH	Tunnel mode with ESP



IPSec Working Details ...



What happens?



What happens?

R1 converts original datagram into IPSec datagram

1. Append to back of original datagram (which includes original header fields!) an „ESP trailer” field.
2. Encrypt result using algorithm and key specified by SA.
3. Append to front of this encrypted quantity the „ESP header”, creating the „envelope”.
4. Create authentication MAC over the whole envelope, using algorithm and key specified in SA;
5. Append MAC to back of envelope, forming payload
6. Create brand new IP header, with all the classic IPv4 header fields, which it appends before payload.

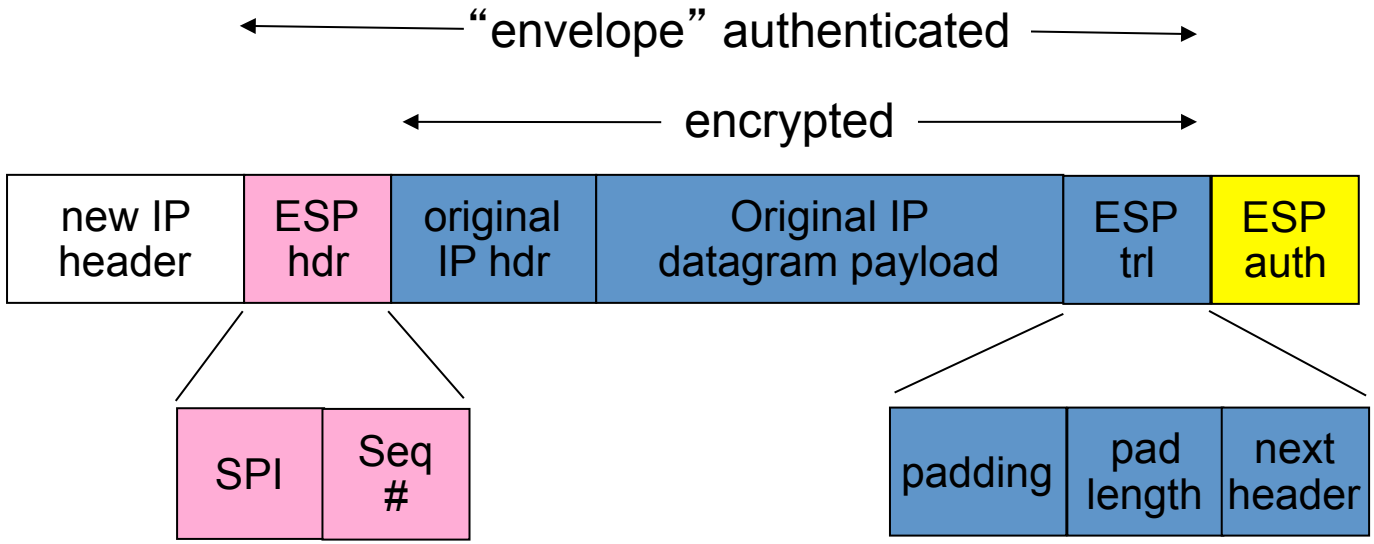
Inside the envelope

ESP trailer: Padding for block ciphers

ESP header:

- SPI, so receiving entity knows what to do
- Sequence number, to thwart replay attacks

MAC in ESP auth field is created with shared secret key



The Encapsulating Security Payload – Fields explained

The SPI field indicates the SA to be used for this packet:

- The SPI value is always determined by the receiving side during SA negotiation as the receiver has to process the packet

The sequence number provides replay protection

If crypto algorithm requires initialization vector, it is transmitted in the clear in every packet in the beginning of the payload

The pad field: padding of the payload up to the required block length of the cipher in use

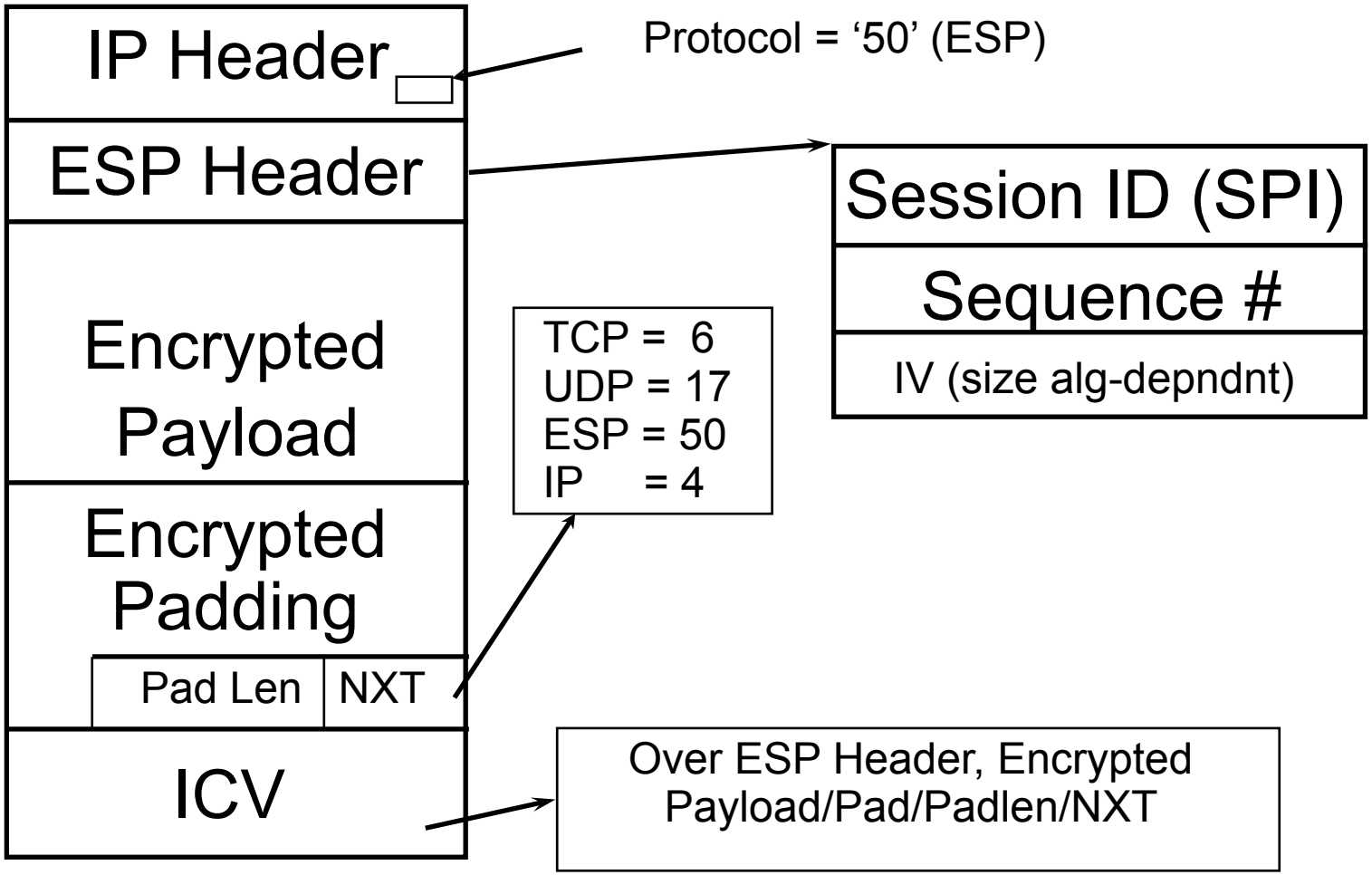
The pad length indicates the amount of padding bytes added

The next-header field of the ESP header indicates the encapsulated payload:

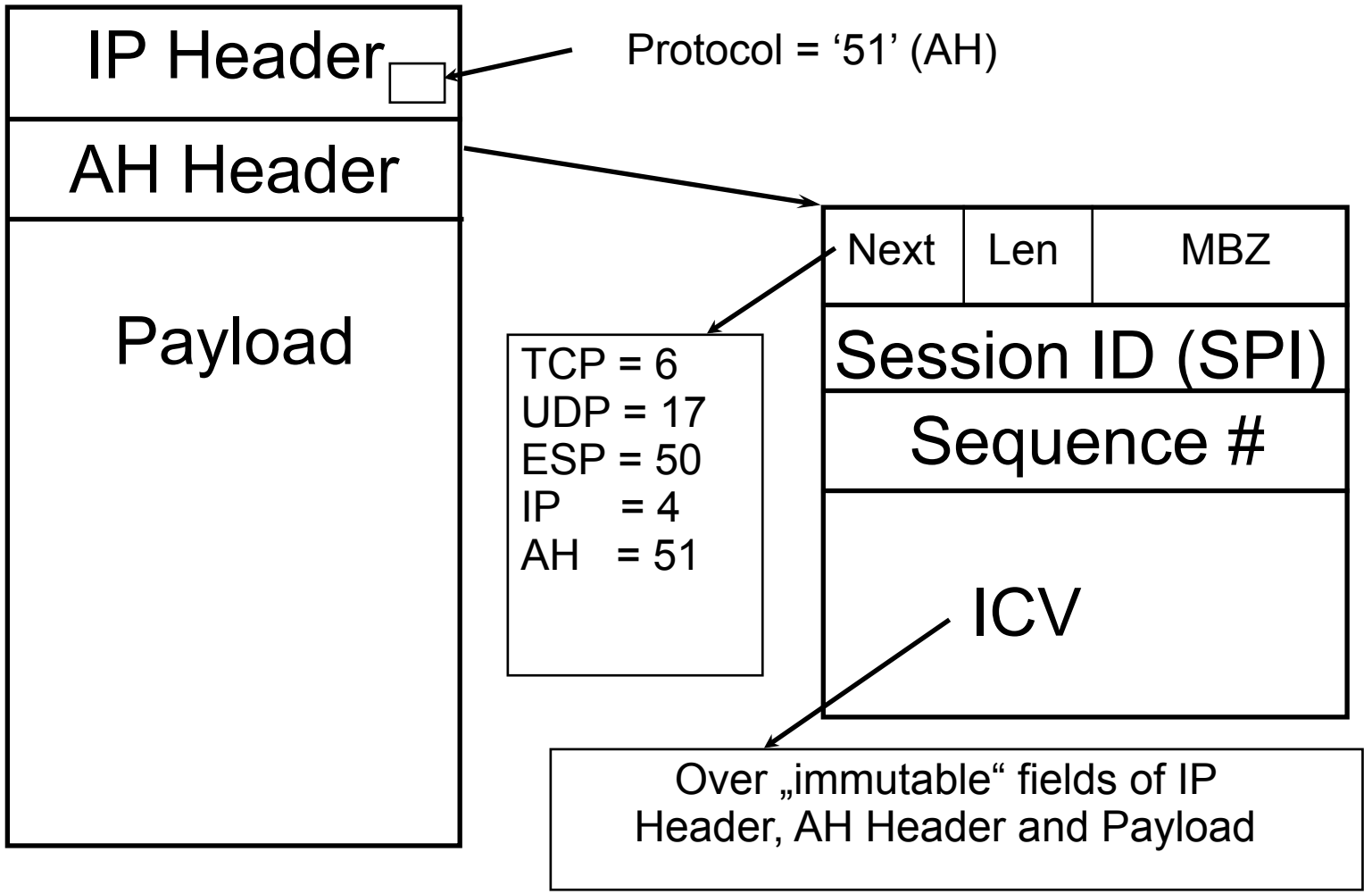
- In case of tunnel mode: IP
- In case of transport mode: any higher-layer protocol as TCP, UDP, ...

The optional authentication-data field contains a MAC, if present

ESP – Transport Mode



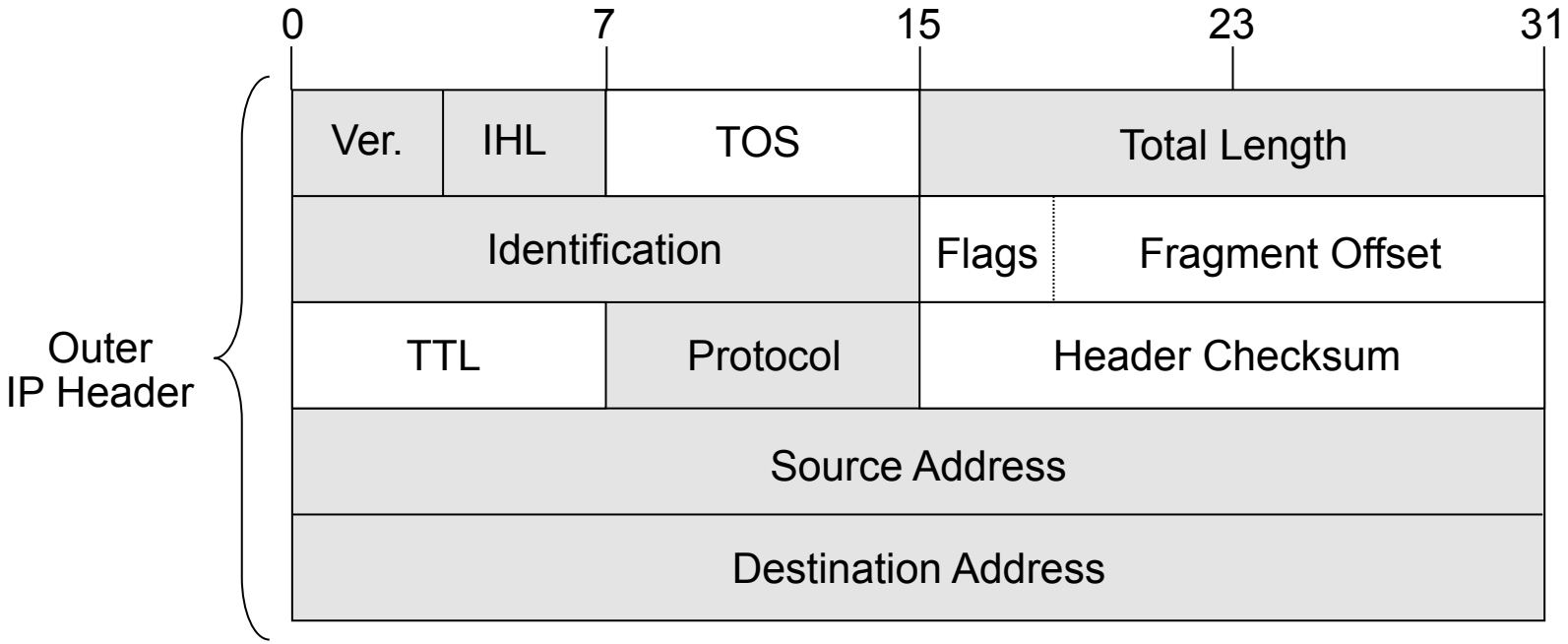
Authentication Header (AH)



Authentication Header (AH)

AH also protects the outer IP header, yet some of its' fields must not be protected as they are subject to change during transit:

- This also applies to mutable IPv4 options or IPv6 extensions
- Such fields are assumed to be zero when computing the MAC



All immutable fields, options and extensions (gray) are protected


HEAVY DUTY
ULTRA STABILIZED

IPSec Sequence Numbers

SECURE MOBILE NETWORKING

Protection against replay

For new SA, sender initializes seq. # to 0

Each time datagram is sent on SA:

- Sender increments seq # counter
- Places value in seq # field

Goal:

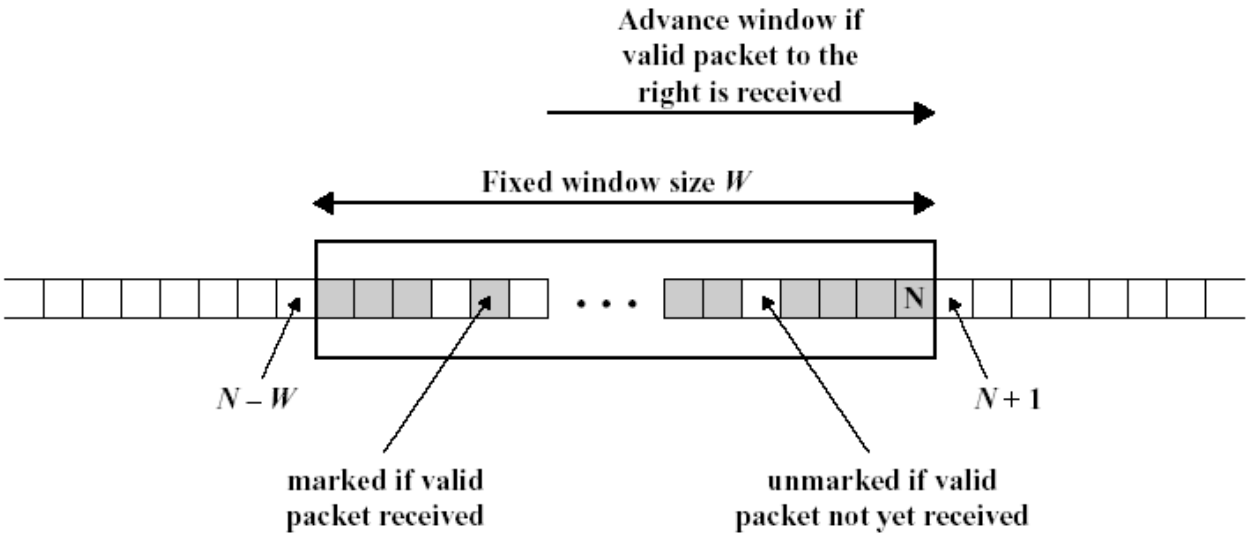
- Prevent attacker from sniffing and replaying a packet
  - Receipt of duplicate, authenticated IP packets may disrupt service

Method:

- Destination checks for duplicates
- But doesn't keep track of ALL received packets; instead uses a window

Algorithm at Receiver

1. If received packet falls in window, packet is new and MAC checks ➜ slot in window marked
2. If received packet is to right of window, MAC check ➜ window advanced & right-most slot marked
3. If received packet is left of window, already marked or fails MAC check ➜ packet is discarded



N is highest sequence # rcvd.

Default W=64

Selected Issues with IPSec

Interoperability problems of end-to-end security with header processing in intermediate nodes:

- Interoperability with firewalls:
  - End-to-end encryption conflicts with the firewalls' need to inspect upper layers protocol headers in IP packets
- Interoperability with network address translation (NAT):
  - Encrypted packets do neither permit analysis nor change of addresses
  - Authenticated packets will be discarded if source or destination address is changed

Conclusion

IPSec is IETF's security architecture for the Internet Protocol

It provides the following security services to IP packets:

- Connectionless integrity
- Data origin authentication
- Confidentiality (encryption)
- Replay protection, access control, limited traffic flow analysis protection

Two fundamental security protocols have been defined:

- Authentication header (AH)
- Encapsulating security payload (ESP)

Operational considerations are necessary (see c05m03):

- SA negotiation and key management
- Inbound and outbound processing of packets


BUT WHEN SHE TRACED THE KILLER'S IP ADDRESS... IT WAS IN THE 192.168/16 BLOCK!
GASP!

Additional References (Standardization Madness)

RFC 2367: PF_KEY Interface
RFC 2401: Security Architecture for the Internet Protocol (IPsec overview) Obsolete by RFC 4301
RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2409: The Internet Key Exchange
RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
RFC 2411: IP Security Document Roadmap
RFC 2412: The OAKLEY Key Determination Protocol
RFC 2451: The ESP CBC-Mode Cipher Algorithms
RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3715: IPsec-Network Address Translation (NAT) Compatibility Requirements
RFC 3947: Negotiation of NAT-Traversal in the IKE
RFC 3948: UDP Encapsulation of IPsec ESP Packets
RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4301: Security Architecture for the Internet Protocol
RFC 4302: IP Authentication Header
RFC 4303: IP Encapsulating Security Payload
RFC 4304: Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
RFC 4306: Internet Key Exchange (IKEv2) Protocol
RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
RFC 4308: Cryptographic Suites for IPsec
RFC 4309: Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
RFC 4543: The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE)
RFC 4621: Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
RFC 4718: IKEv2 Clarifications and Implementation Guidelines
RFC 4806: Online Certificate Status Protocol (OCSP) Extensions to IKEv2
RFC 4809: Requirements for an IPsec Certificate Management Profile
RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4945: The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

Acknowledgements

Selected slides of this chapter courtesy of

- Keith Ross, Steven Kent with changes of myself incorporated
- Some other slides courtesy of G. Schäfer (TU Ilmenau) with changes of J. Schmitt (TU Kaiserslautern) and myself incorporated
- Yet some other slides courtesy of R. Perlman, K. Ross, Y. Chen, W. Stallings (L. Brown); changes of myself incorporated
- Some slides my Marc Werner, SEEMOO

Images taken from:

- www.pixelio.de
- www.renault.fr
- view.stern.de
- www.xkcd.org
- www.bl.uk

Recommended Reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6

- [Stallings2011] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2011, ISBN: 978-0-136-10805-4

- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

Copyright Notice