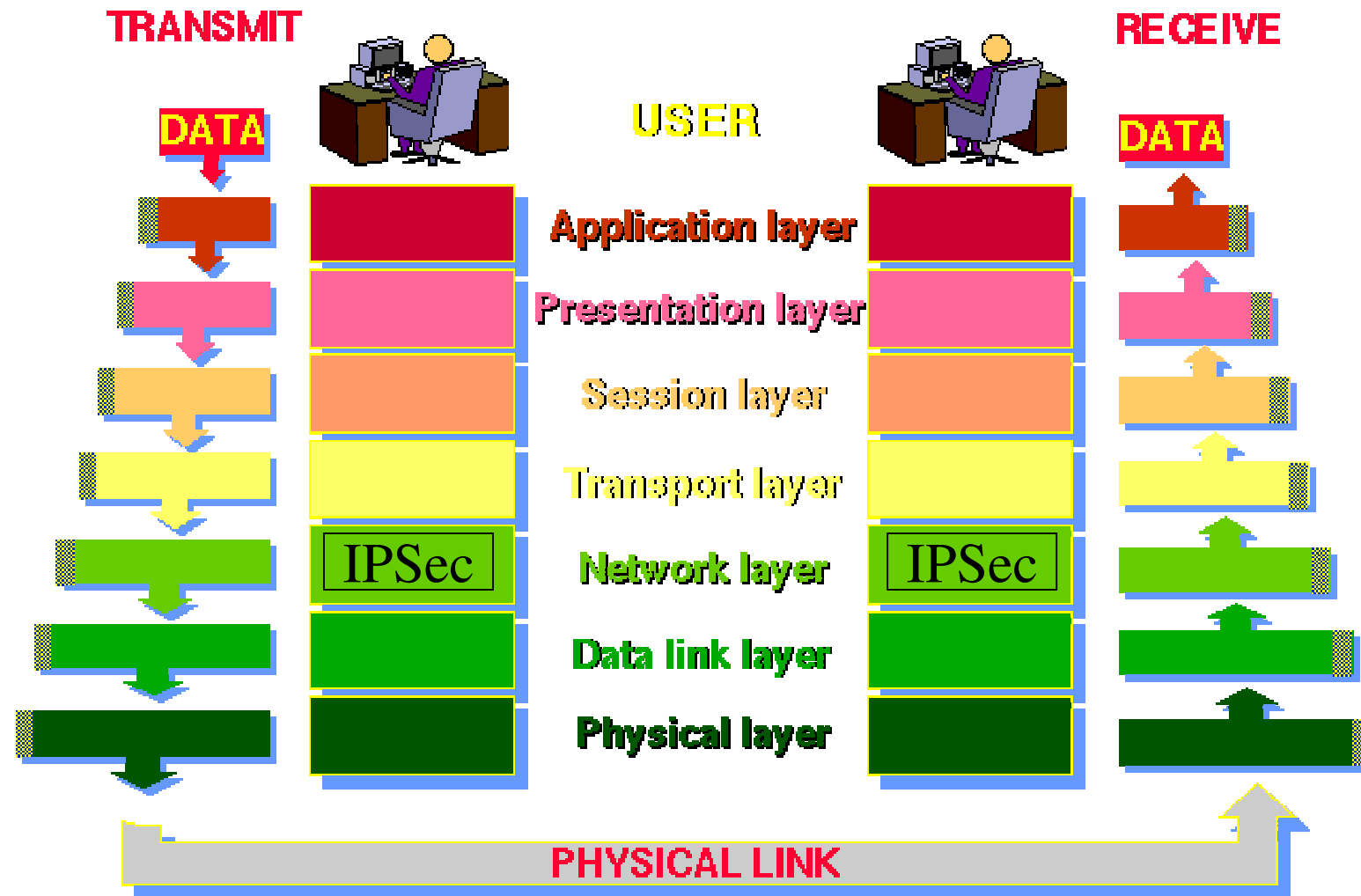


Written by Daniel Butt

IPSec: What is it?

- Internet Protocol Security
- Provides secure exchange / encryption of packets
- Functions on the Network Layer

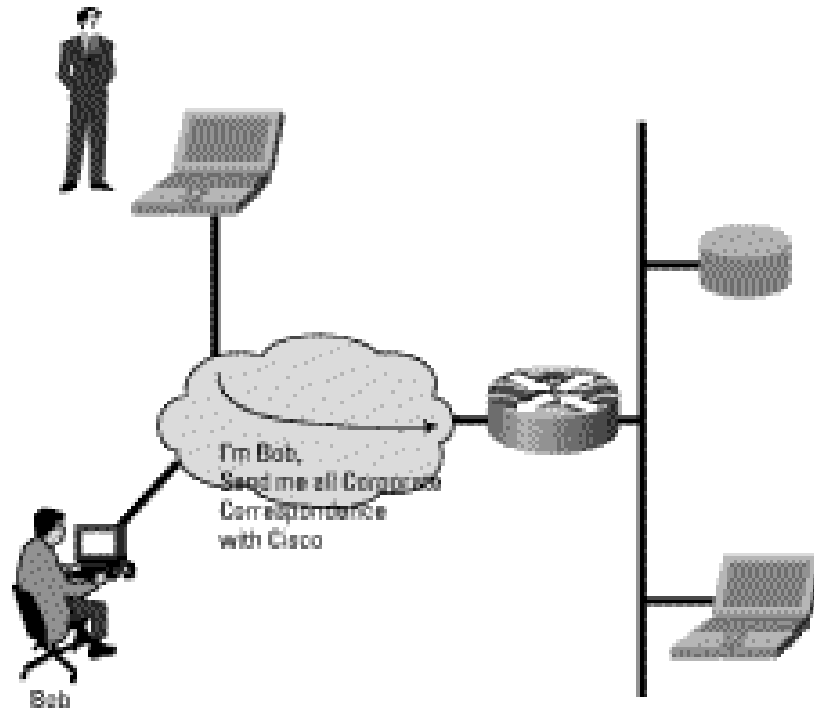
THE 7 LAYERS OF OSI



Why Do We Need It?

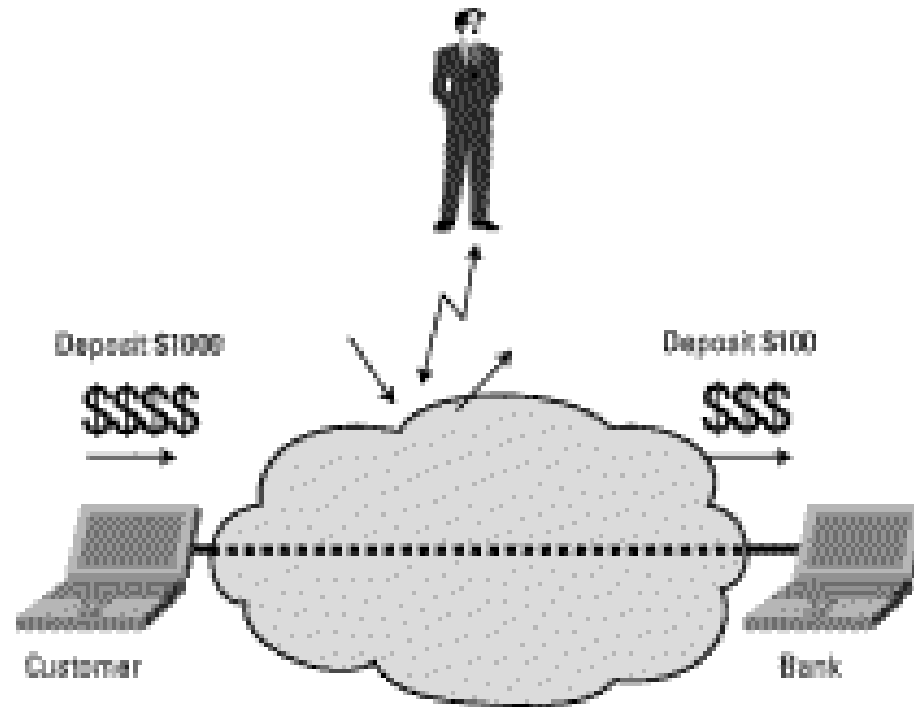
- IP is insecure
- Weaknesses of:
 - Source Authentication
 - Data Integrity
 - Message Confidentiality
 - Packet Replay

Authentication



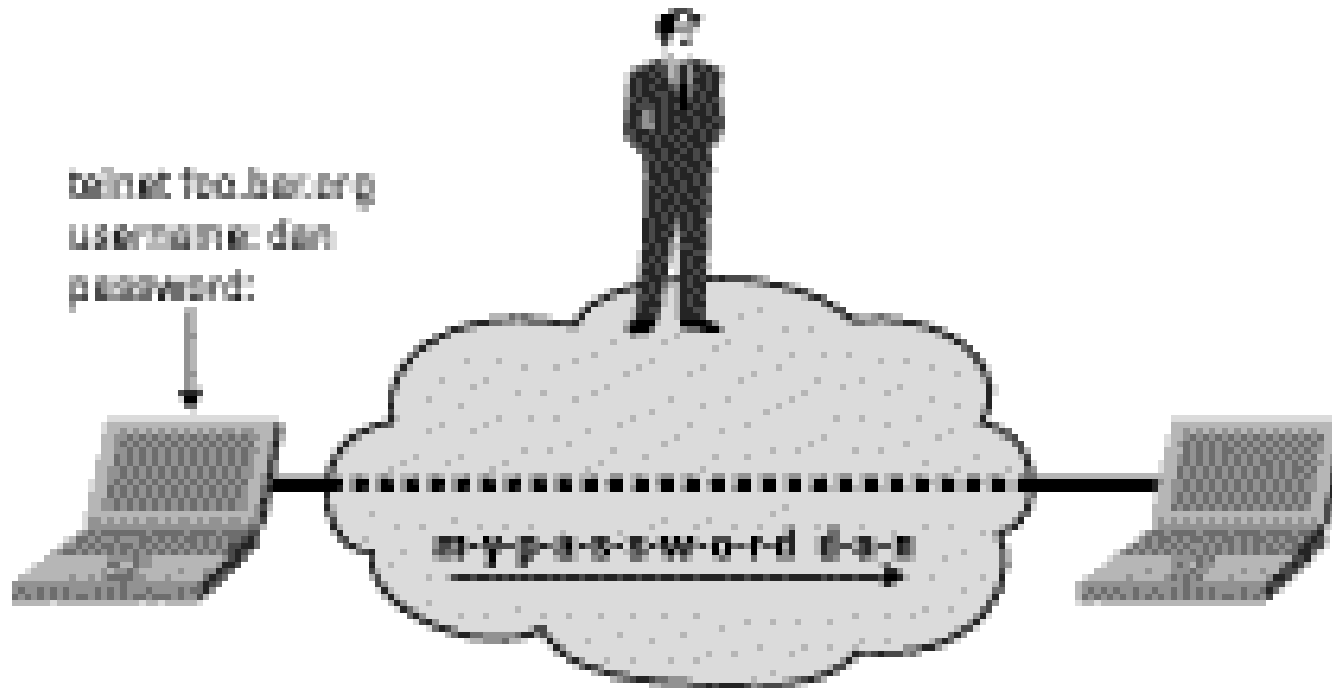
How do you know the sender is actually who they claim to be?

Integrity



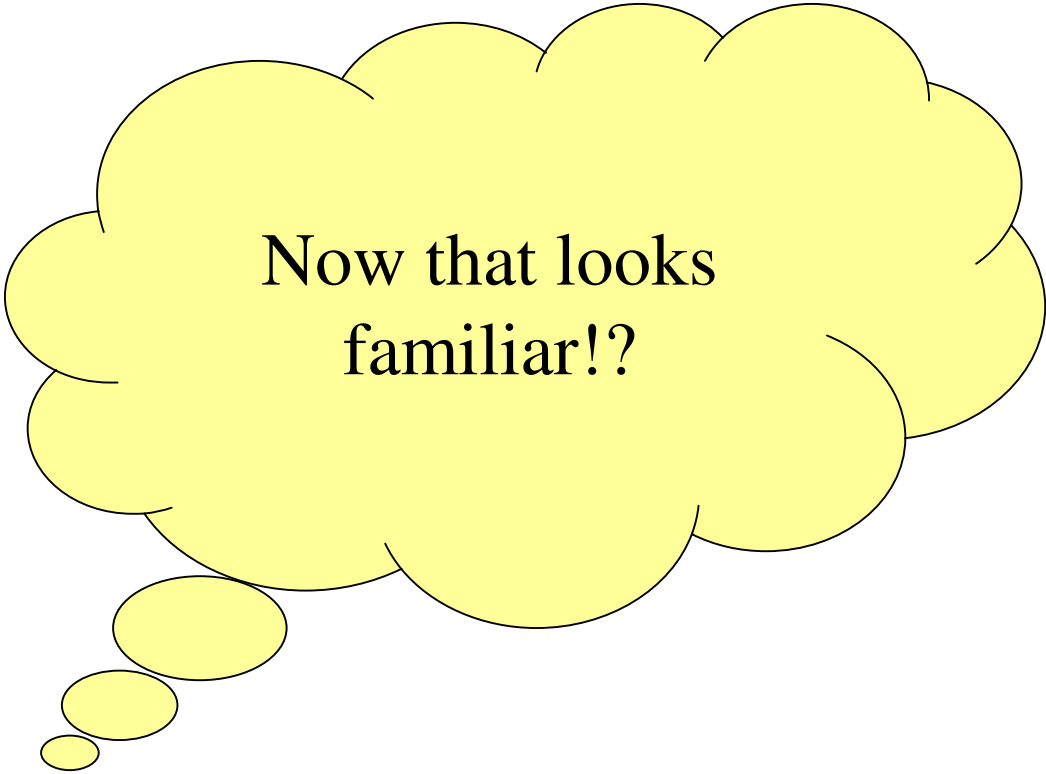
How do you know the data received is in fact what was sent?

Confidentiality



How do you know the intended recipient is the only person reading the message?

Replay



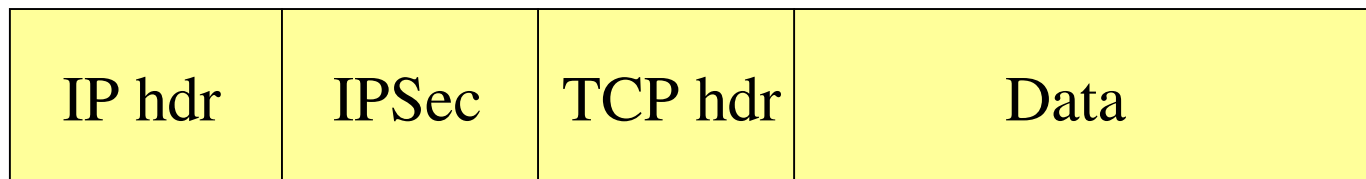
Now that looks
familiar!?

How is it Implemented?

- RFC 2401-2411
- 2 Modes of operation
 - Transport Mode
 - Tunnel Mode
- 2 Basic Security protocols
 - Authentication header (AH)
 - Encapsulating Security Payload (ESP)
- Can be implemented on an ‘end host’ or ‘gateway’

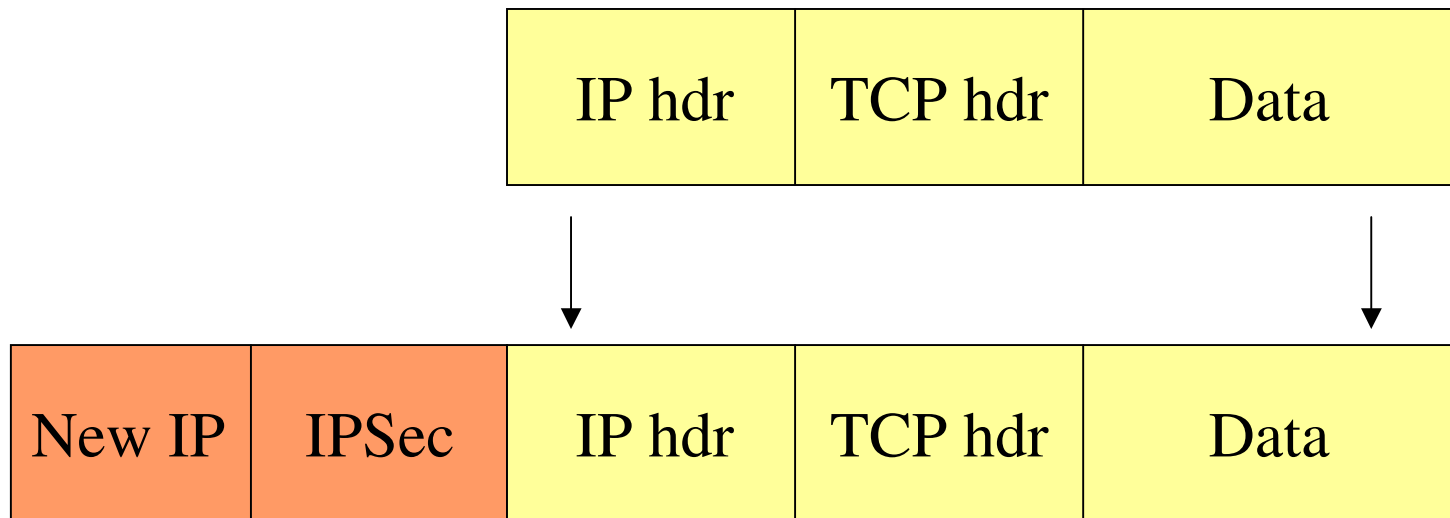
Transport Mode

- IPSec information is inserted after the original IP Header
- Only the transport layer information has IPSec protection



Tunnel Mode

- IPSec encapsulates the original datagram within a new packet



Authentication Header

- *“used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays”*

– RFC2402

- AH is defined in the packet by the number 51 in the Protocol field

AH Packet Analysis

- Next Header
 - Identifies type of next payload after AH
 - I.e. TCP, ICMP etc
- Payload Length
 - Length of the AH
- Reserved
 - Reserved for future use
 - Must be set to zero

AH Packet Analysis (cont)

- Security Parameters Index
 - A number that is used to distinguish the SA
 - I.e. used to uniquely identify the session
- Sequence Number
 - Used for Replay Protection
- Authentication Data
 - Contains Integrity Check Value
 - Calculated by using an algorithm such as a hash function

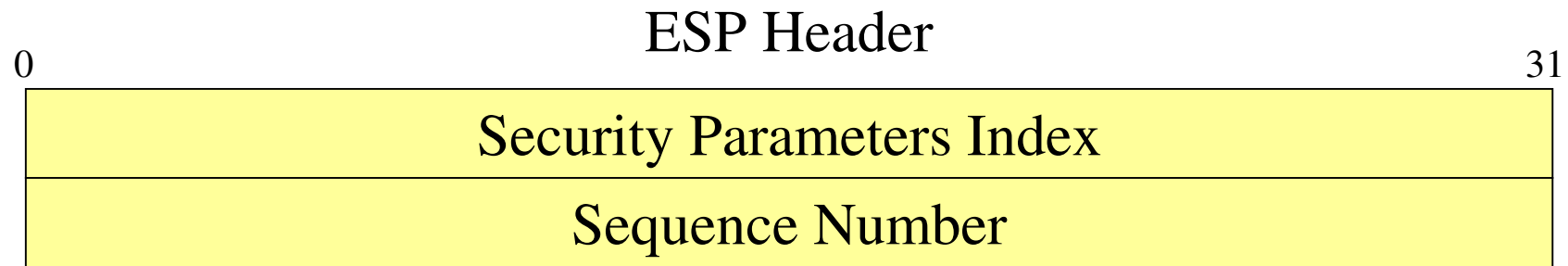
Integrity Check Value Calculation

- IP packet is divided into mutable, immutable and predictable fields
- Only those classed as immutable and predictable are used
- The mutable fields are set to 0, to preserve alignment

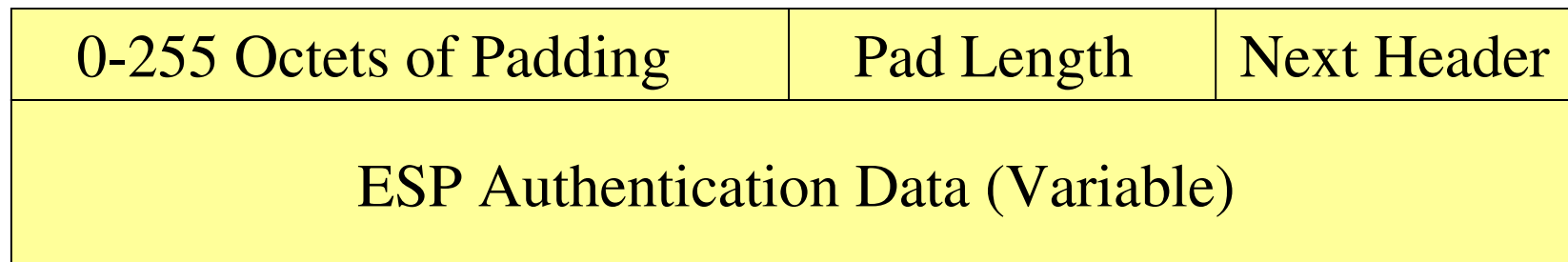
Encapsulating Security Payload

- Handles privacy as well as authentication
- AH is defined in the packet by the number 51 in the Protocol field
- ESP adds 3 additional areas to the packet
 - ESP Header
 - ESP Trailer
 - ESP Authentication

ESP Packet Structure

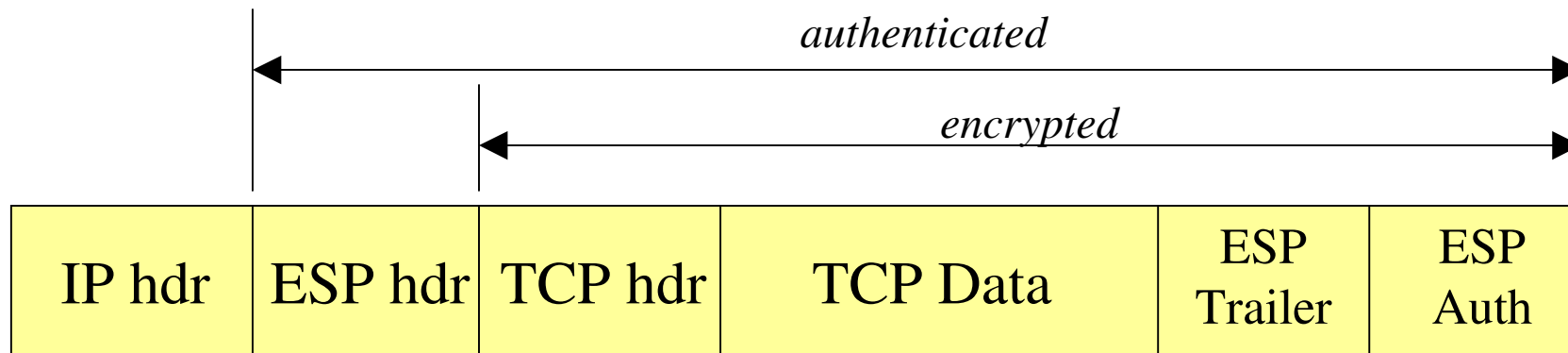


ESP Trailer and Authentication



ESP Packet Structure (cont)

Authentication and Encryption division



ESP Packet Analysis

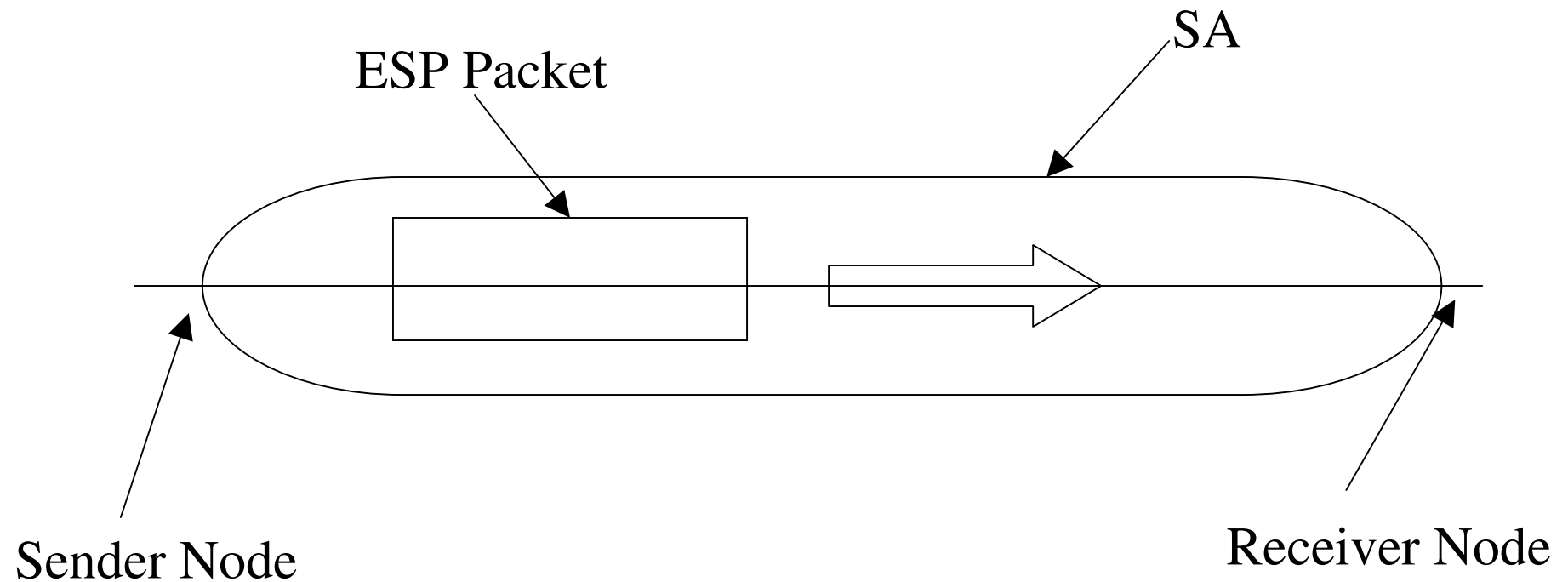
- Security Parameters Index (SPI)
 - Same as in AH
- Sequence Number
 - Same as in AH
- Padding
 - Some encryption algorithms require plaintext to be a fixed size (block cipher)
 - Also Pad Length and Next header must be right aligned

ESP Packet Analysis (cont)

- Pad Length
 - Number of bytes padding uses
- Next Header
 - Same is in AH
- ESP Authentication data
 - Optional field in ESP

Security Association (SA)

- A one-way connection that affords security services to the traffic carried by it (AH or ESP)



SA (cont)

- Uniquely identified by:
 - SPI, IP Destination address, Security Protocol
- Essential Elements of SA:
 - Security Policy Database (SPD)
 - Security Association Database (SAD)

Security Policy Database

- All inbound and outbound traffic must be presented to SPD
- SPD decides whether packets are:
 - IPSec protected
 - Allowed to bypass IPSec
 - Discarded

Security Association Database

- Each entry defines parameters associated with one SA
- Parameters include:
 - IPSec protocols
 - Modes (transport or tunnel)
 - Authentication/Encryption algorithms used
 - Lifetime of the SA

Security Algorithms

- Integrity Checks using message digests
 - HMAC with MD5
 - HMAC with SHA-1
- Encryption
 - DES

Weaknesses of IPSec

- An argument of complexity
- Only as strong as the encryption protocols that make it

Applied Uses

- On a host machine or a gateway
- LAN secure communication
- VPN's (Virtual Private Networks)
 - Secure communication over the Internet