Securing Wireless Networks, COMP4337/9337
WK04: Network Layer Security: IPsec

Never Stand Still

Professor Sanjay K. Jha

School of Computer Science and Engineering, UNSW

Why Network Layer Security?

- Higher-layer security mechanisms do not necessarily protect an organisation's internal network links from malicious traffic.
- If and when malicious traffic is detected at the end-hosts, it is too late, 高层协议并不能兼顾到底层安全
  - bandwidth has already been consumed.
- Higher-layer security mechanisms (e.g., TLS) do not conceal IP headers.
  - IP addresses of the communicating end-hosts visible to eavesdroppers.
- Possible to create Secure VPN (more soon)

What is network-layer confidentiality ?

between two network entities:

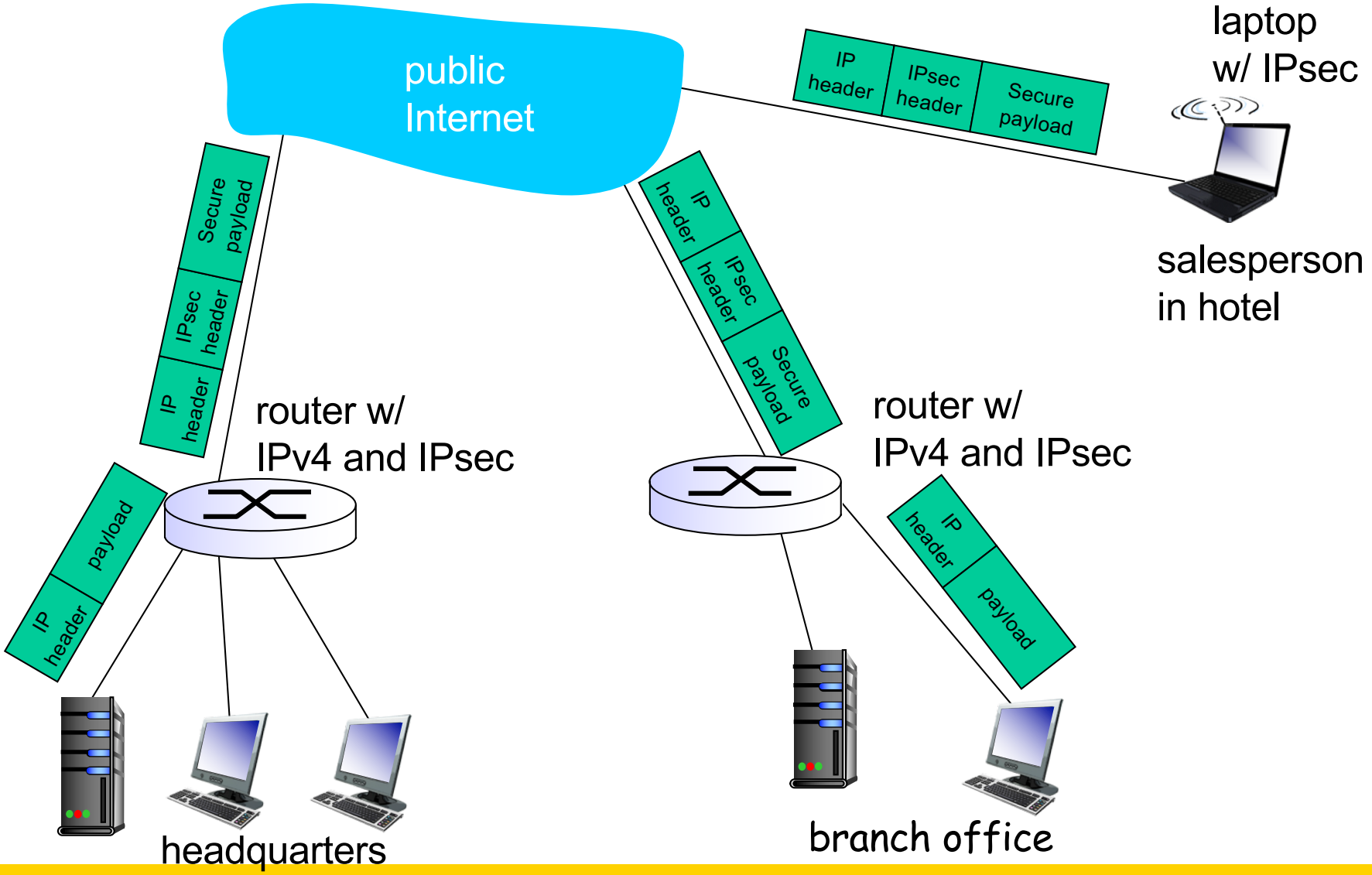
- sending entity encrypts datagram payload, payload could be:
  - TCP or UDP segment, ICMP message, OSPF message ….
    - Implemented below Transport layer (TCP/UDP)
    - Even when implmented in end-systems, doesn't affect higher layers
- all data sent from one entity to other would be hidden:
  - web pages, e-mail, P2P file transfers, TCP SYN packets …
- "blanket coverage"

Virtual Private Networks (VPNs)

motivation:

- institutions often want private networks for security.
  - costly: separate routers, links, DNS infrastructure.
- VPN: institution's inter-office traffic is sent over public Internet instead
  - encrypted before entering public Internet
  - logically separate from other traffic

Virtual Private Networks (VPNs)



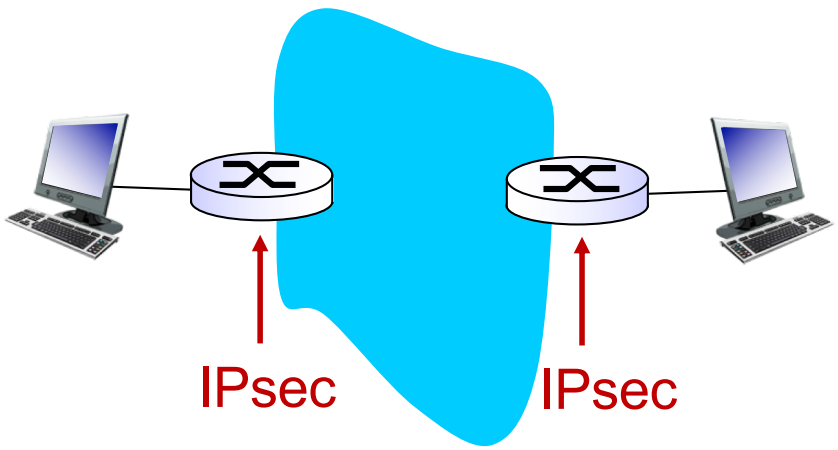
IPsec services

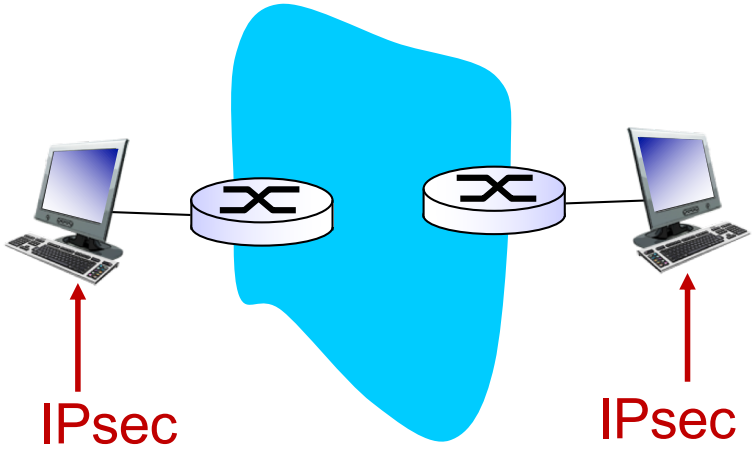
- Data integrity
- Origin authentication
- Replay attack prevention
- Confidentiality
- Two different offerings (AH and ESP) discussed later

Tunnel and Transport Modes

- Transport Mode: protects IP Payload received from layers above (Higher layer TCP, UDP, ICMP..)
  - There are many detailed nuances with AH/ESP support, encapsulation etc.
- Tunnel Mode: All of IP including header etc is encapsulated, new IP header is added by Firewall/Routers.
  - End hosts behind firewall don't have to worry about IPSec
  - We will focus on Tunnel Mode here as it is more widely used

IPsec – tunneling mode





- edge routers IPsec-aware
  - IP address of Routers/Gateways used, destination address encrypted
- hosts IPsec-aware
- Also possible that one host is IPSec aware and other behind firewall

Advantages of tunnel mode (Edge)

- Simple key distribution: fewer keys needed as gateways do encryption/decryption
- Traffic analysis difficult as ultimate destination IP header concealed
- Less processing burden on end-hosts

- **OPTIONAL READ:** C. Kiraly, S. Teofili, G. Bianchi, R. Lo Cigno, M. Nardelli, and E. Delzeri, "Traffic flow confidentiality in IPsec: Protocol and implementation," in The Future of Identity in the Information Society, S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, Eds. Boston, MA:

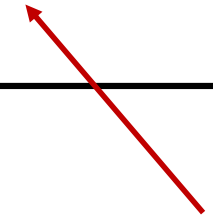
  Springer US,2008, pp. 311–324.

Two IPsec protocols

- Authentication Header (AH) protocol
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP)
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

Four combinations are possible!

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



most common and most important

Protocol Operations for ESP

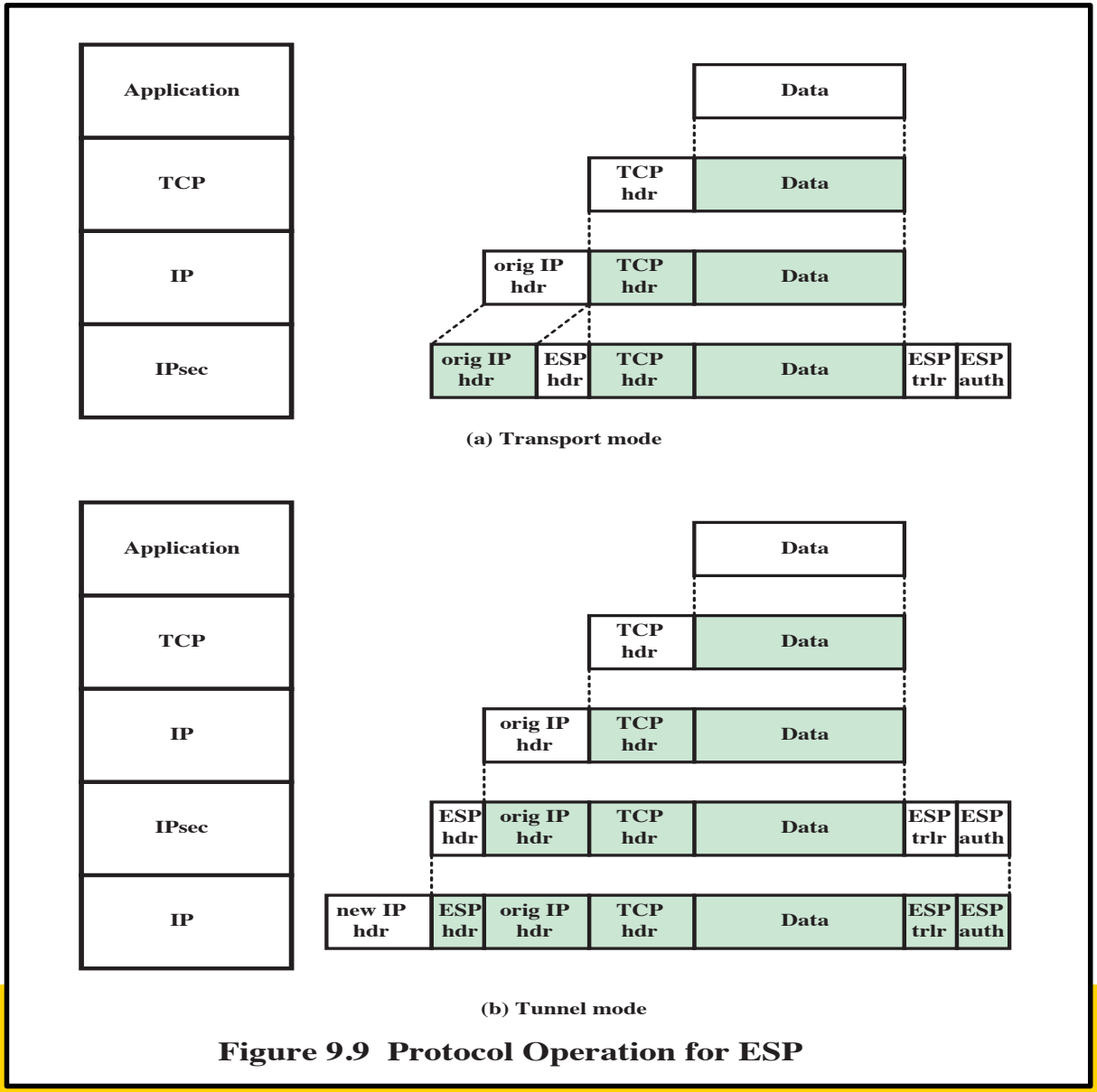


Figure 9.9 Protocol Operation for ESP

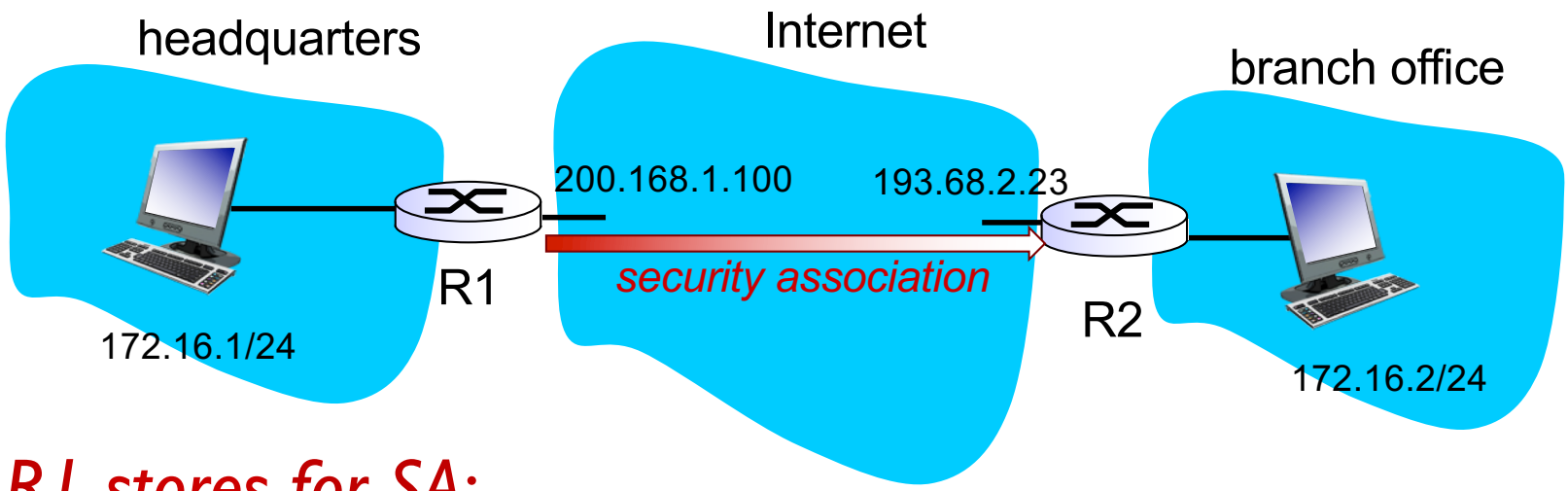
Transport:
Original IP Hdr

Tunnel
New IP Hdr

Security associations (SAs)

- before sending data, "security association (SA)" established from sending to receiving entity
  - SAs are simplex: for only one direction
- ending, receiving entitles maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; ***IPsec is connection-oriented!***
- *Combination of Security Associations has many advanced features : Read stallings Chapter9 (not examinable)*

Example SA from R1 to R2



R1 stores for SA:

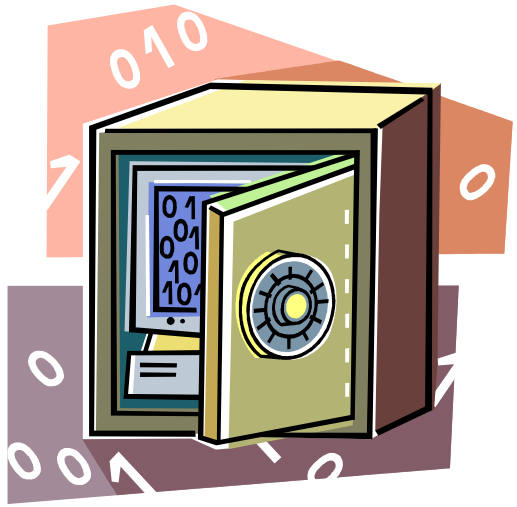
- 32-bit SA identifier: *Security Parameter Index (SPI)* exam
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used (e.g., 3DES with CBC)
- encryption key
- type of integrity check used (e.g., HMAC with MD5)
- authentication key

Security Association Database (SAD)

- endpoint holds SA state in *security association database (SAD)*, where it can locate them during processing.
- when sending IPsec datagram, R1 accesses SAD to determine how to process datagram.
- when IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, and processes datagram accordingly.

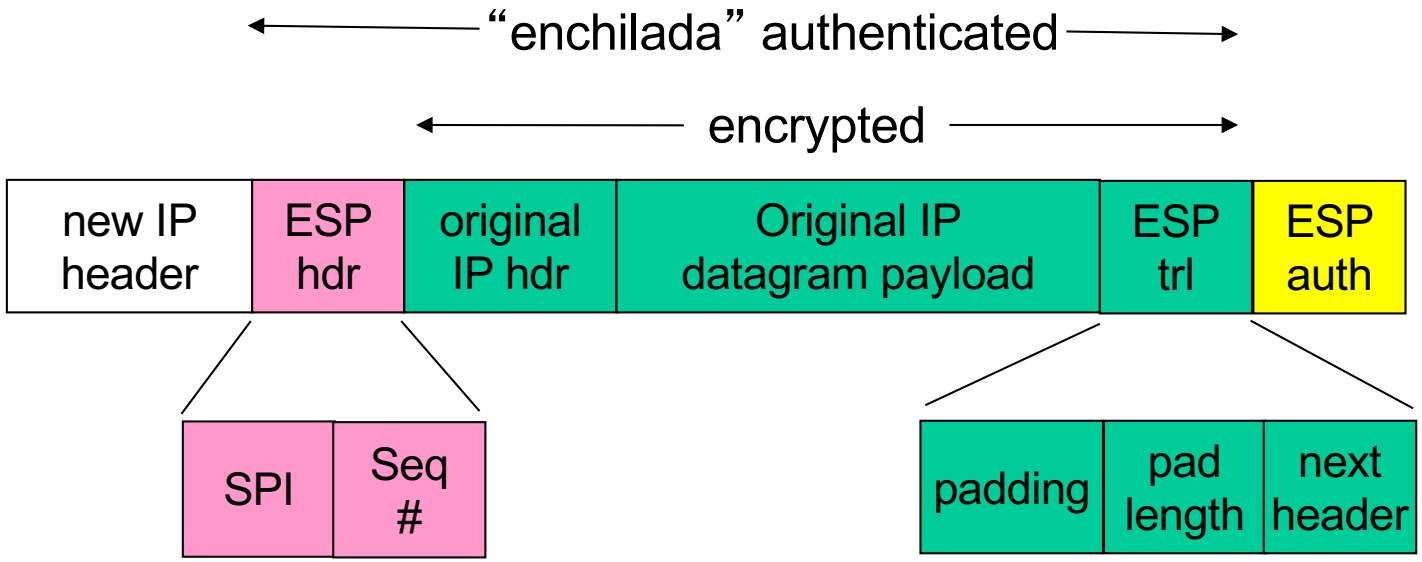
SAD Parameters

- Normally defined by the following parameters in a SAD entry:
  - Security parameter index
  - Sequence number counter
  - Sequence counter overflow
  - Anti-replay window
  - AH information
  - ESP information
  - Lifetime of this security association
  - IPsec protocol mode
  - Path MTU



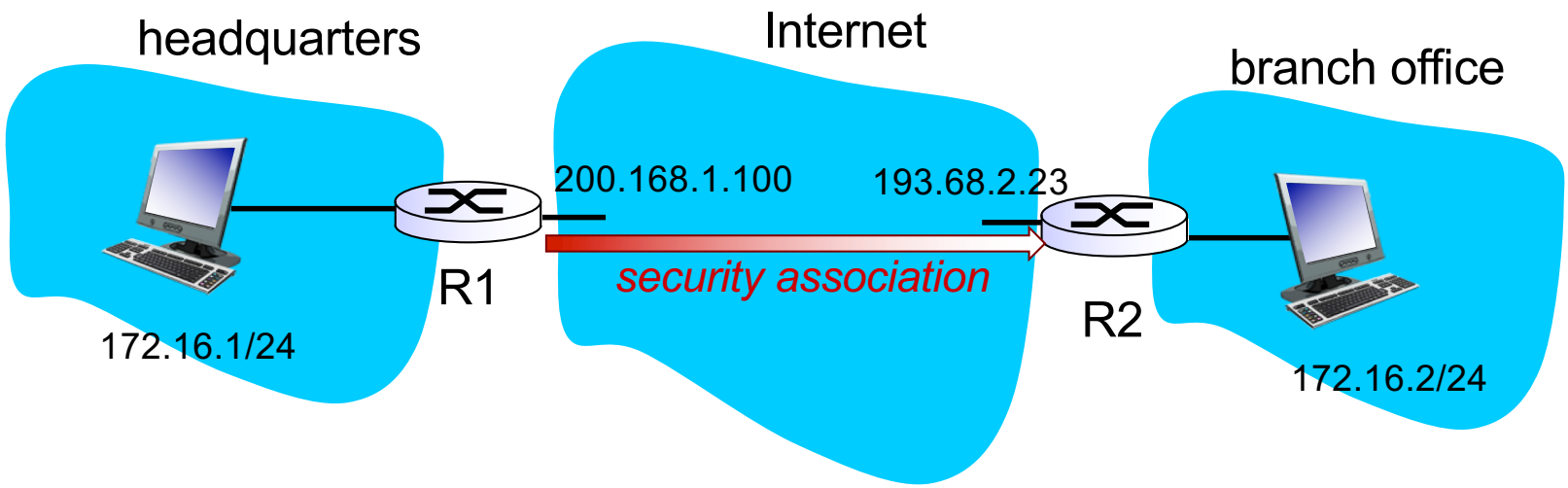
IPsec datagram

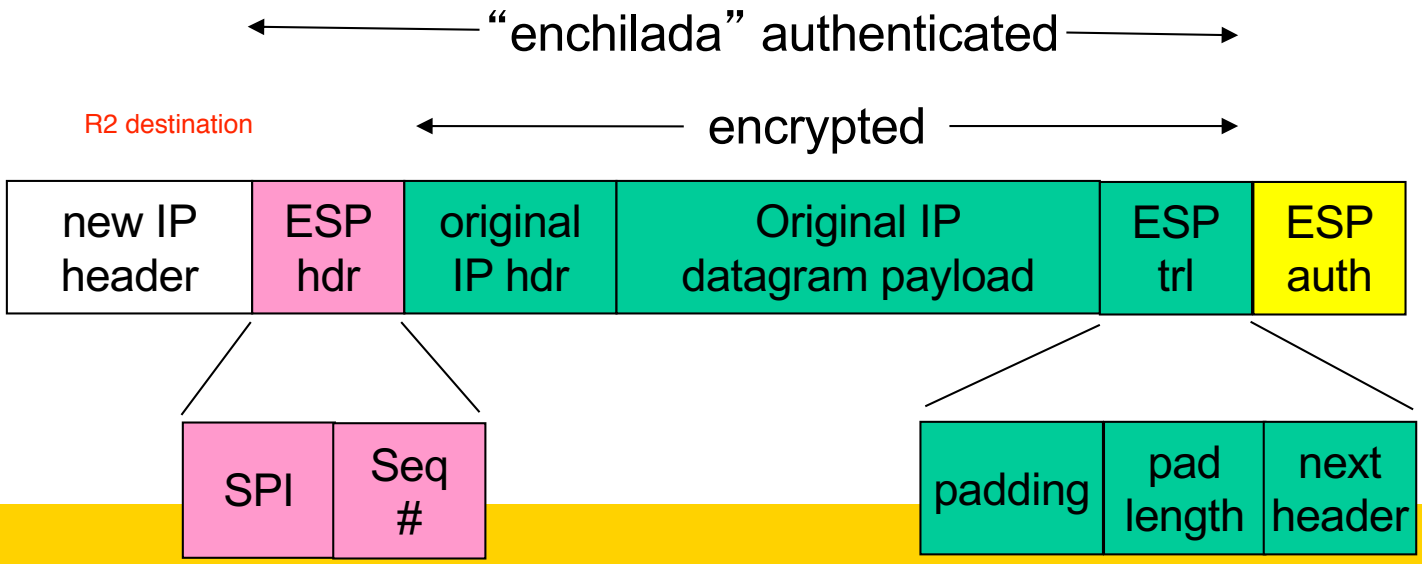
focus for now on tunnel mode with ESP



Note; Original IP address/hdr encrypted, destination Router/GW

What happens?

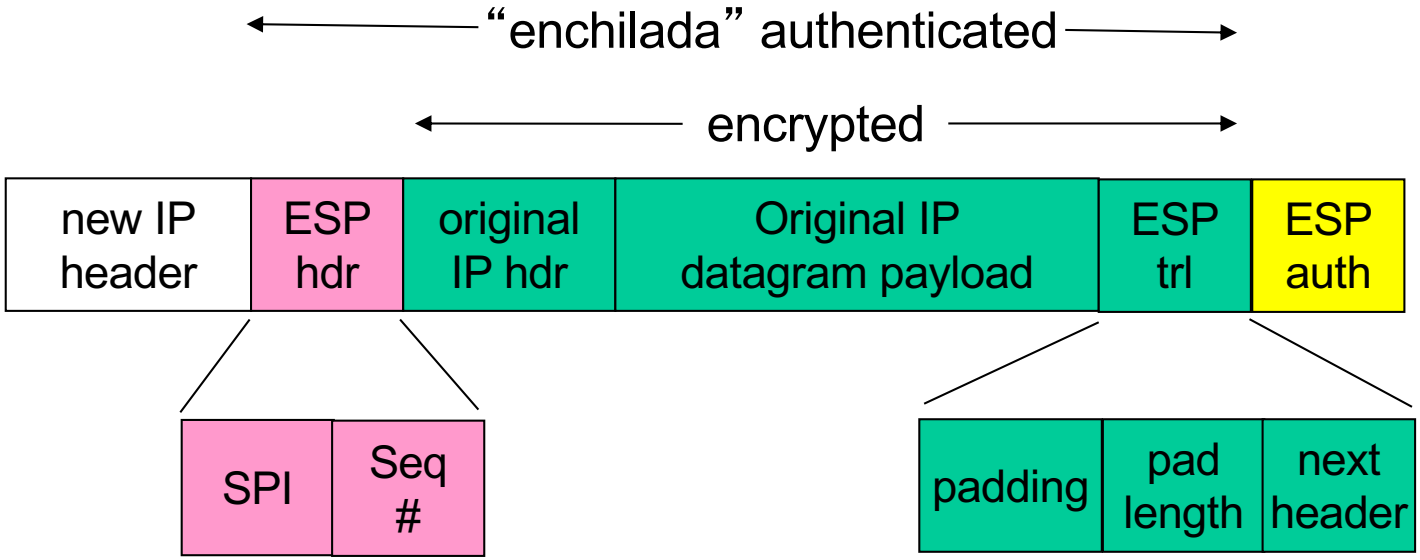




R1: convert original datagram to IPsec datagram

- appends to back of original datagram (which includes original header fields!) an "ESP trailer" field.
- encrypts result using algorithm & key specified by SA.
- appends to front of this encrypted quantity the "ESP header, creating "enchilada".
- creates authentication MAC over the *whole enchilada*, using algorithm and key specified in SA;
- appends MAC to back of enchilada, forming *payload*;
- creates brand new IP header, with all the classic IPv4 header fields, which it appends before payload.

Inside the enchilada:



- 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 (HMAC)
  - Note: ESP header is included in MAC calculation

security association (SA)An SA is a relationship between two or more entities that describes how the entities will use security services to communicate securely

IPsec sequence numbers

- 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
    - doesn't keep track of *all* received packets; instead uses a window (remember from 3331)

Security Policy Database (SPD)

- policy: For a given datagram, sending entity needs to know if it should use IPsec
- needs also to know which SA to use
  - may use: source and destination IP address; protocol number
- info in SPD indicates "what" to do with arriving datagram
- info in SAD indicates "how" to do it

https://doc.hcc-embedded.com/display/INICHEIPSECANDIKE/Security+Policy+Database

Host SPD Example

Security Policy Database

一种存有policy的数据库

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Src: Stallings. Table9.2

Notes on Table 9.2

Table 9.2 provides an example of an SPD on a host system (as opposed to a network system such as a firewall or router). This table reflects the following configuration:

A local network configuration consists of two networks. The basic corporate network configuration has the IP network number 1.2.3.0/24. The local configuration also includes a secure LAN, often known as a DMZ, that is identified as 1.2.4.0/24. The DMZ is protected from both the outside world and the rest of the corporate LAN by firewalls. The host in this example has the IP address 1.2.3.10, and it is authorized to connect to the server 1.2.4.10 in the DMZ.

The entries in the SPD should be self-explanatory. For example, UDP port 500 is the designated port for IKE. Any traffic from the local host to a remote host for purposes of an IKE exchange bypasses the IPsec processing.

IPsec Outbound Processing

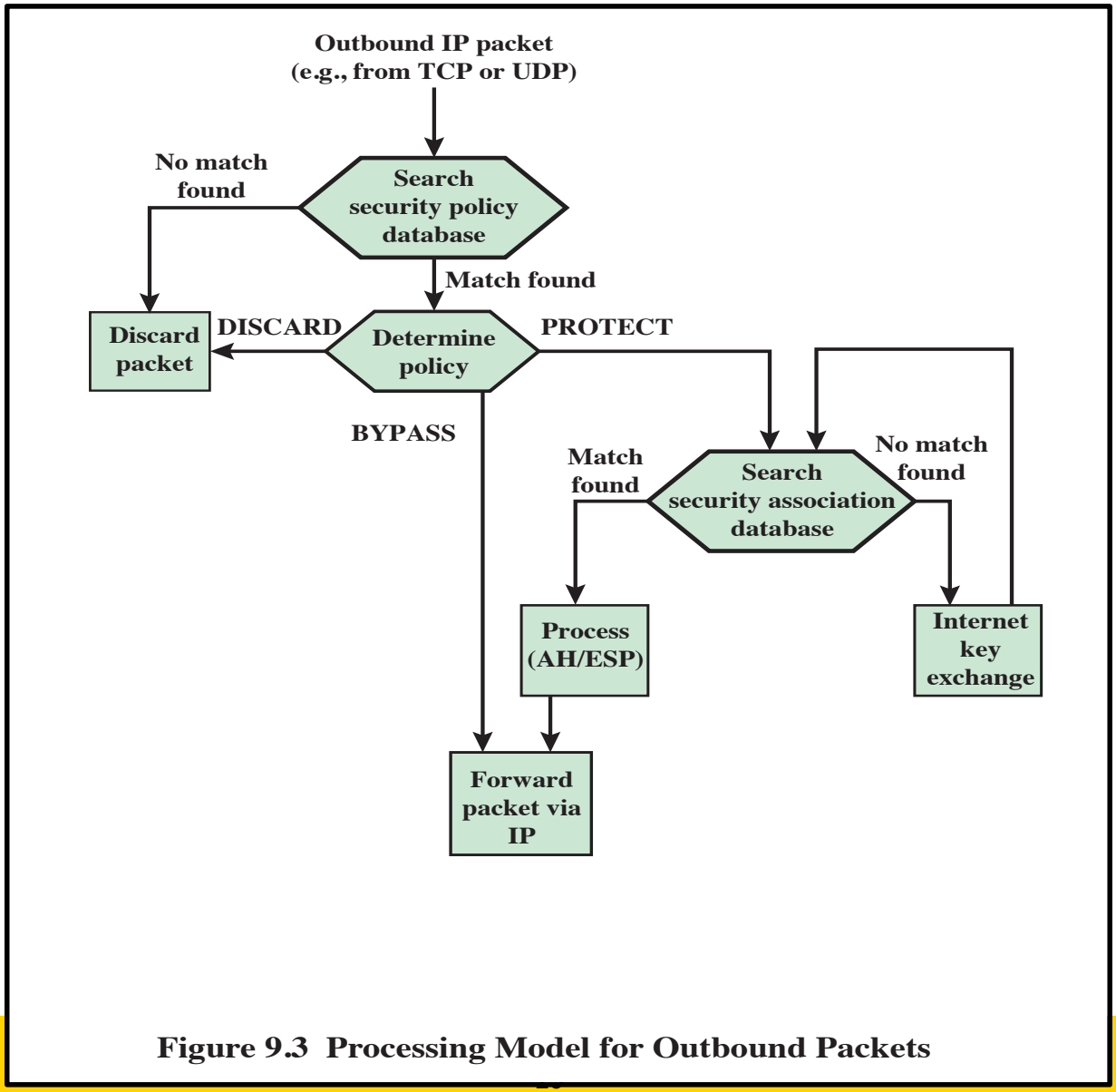


Figure 9.3 Processing Model for Outbound Packets

IPsec Inbound Processing

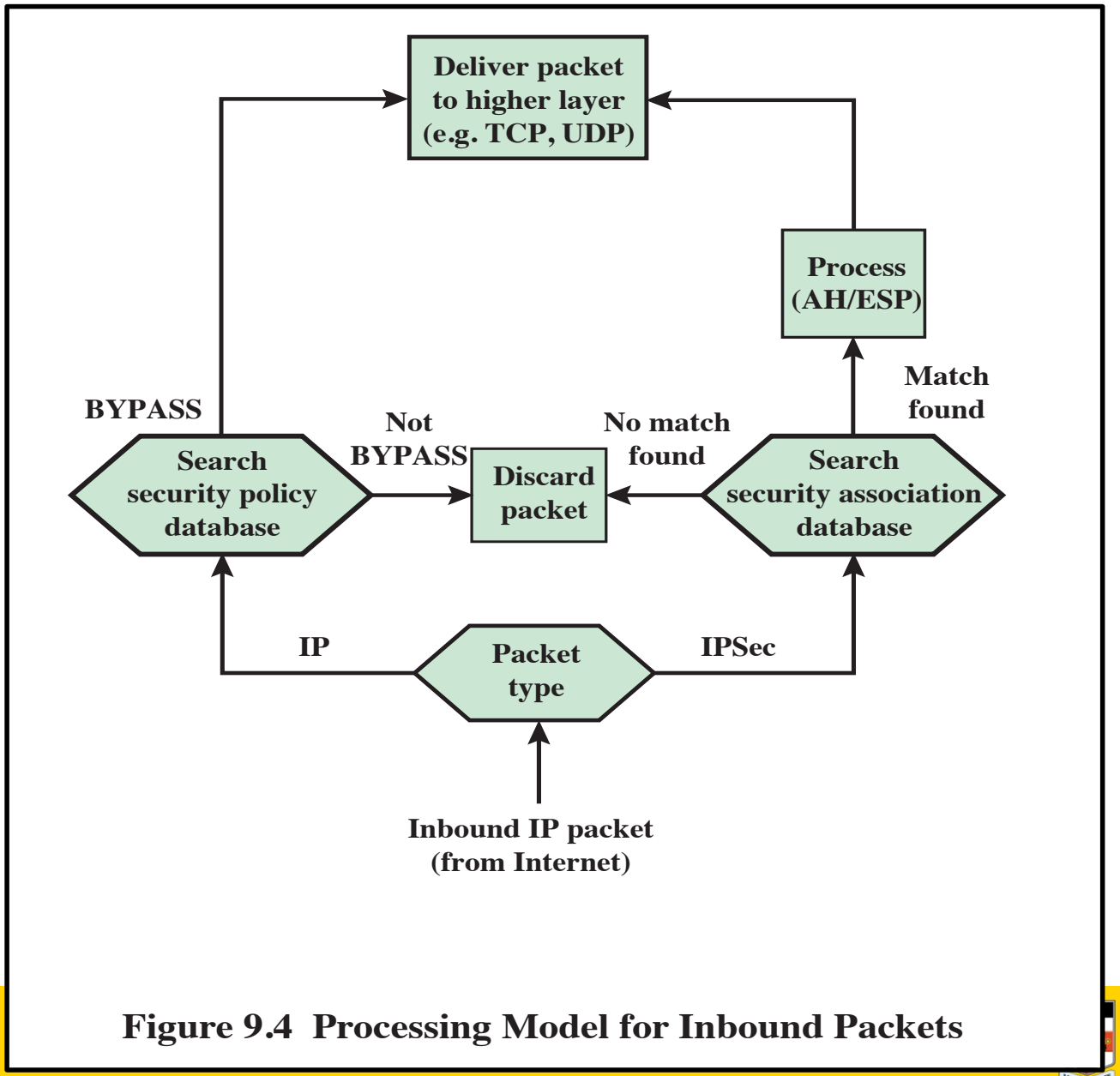


Figure 9.4 Processing Model for Inbound Packets

not exam

IKE: Internet Key Exchange

- *previous examples:* manual establishment of IPsec SAs in IPsec endpoints:

  Example SA

  SPI: 12345
  Source IP: 200.168.1.100
  Dest IP: 193.68.2.23
  Protocol: ESP
  Encryption algorithm: 3DES-cbc
  HMAC algorithm: MD5
  Encryption key: 0x7aeaca…
  HMAC key:0xc0291f…

- manual keying is impractical for VPN with 100s of endpoints
- instead use *IPsec IKE (Internet Key Exchange) RFC5996*

IPsec summary

- IKE message exchange for algorithms, secret keys, SPI numbers
- either AH or ESP protocol (or both)
  - AH provides integrity, source authentication
  - ESP protocol (with AH) additionally provides encryption
- IPsec peers can be two end systems, two routers/firewalls, or a router/firewall and an end system

Reference

- Section 8.7, Computer Networking A top-Down Approach: Jim Kurose and Keith Ross, Chapter 8, (foils provided by Authors): Section 9.2 and 9.5 Network Security Essentials: Stallings: Cybok Network Security KA – Section 5
- **NOTE:**
  - Internet Key Exchange is a Optional reading. Not covered in lecture as ideas are similar to SSL.
  - Additional foils on AH and Tunnel modes are provided for optional reading. AH mode is supported for backward compatibility only. Many complicated features not covered.

Authentication Header (AH)

- AH provides ***authentication*** but not ***privacy***
- a special hashing algorithm and a specific key known only to the source and the destination used to generate authentication header
- Parts of the datagram used for the calculation, and the placement of the header, depends on the mode (tunnel or transport) and the version of IP (IPv4 or IPv6)
- Details at https://tools.ietf.org/html/rfc4302

AH Header

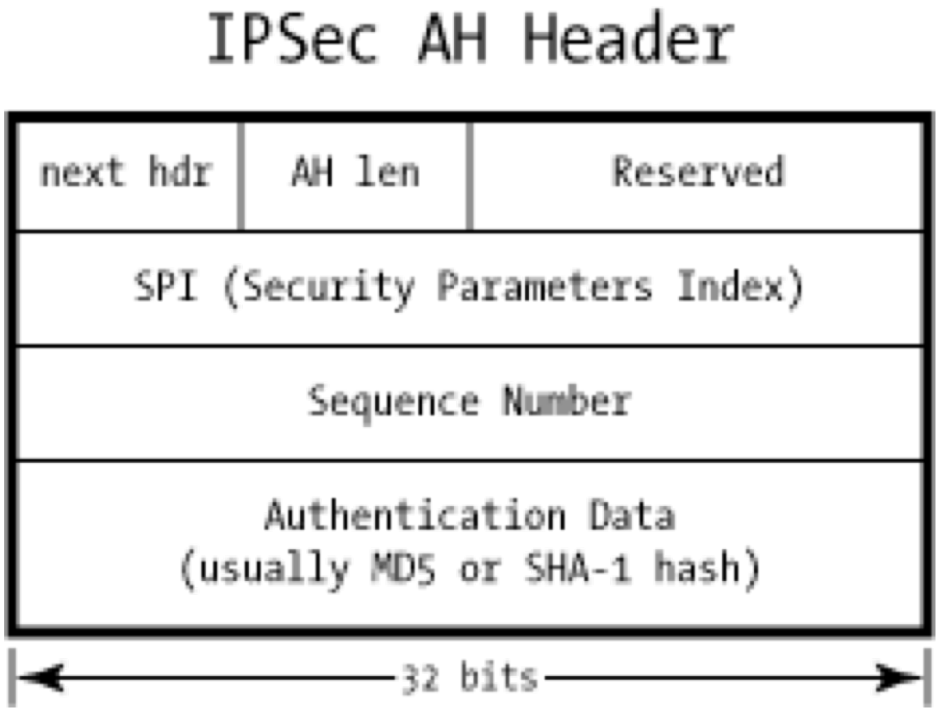


Figure src: http://www.unixwiz.net/techtips/iguide-ipsec.html

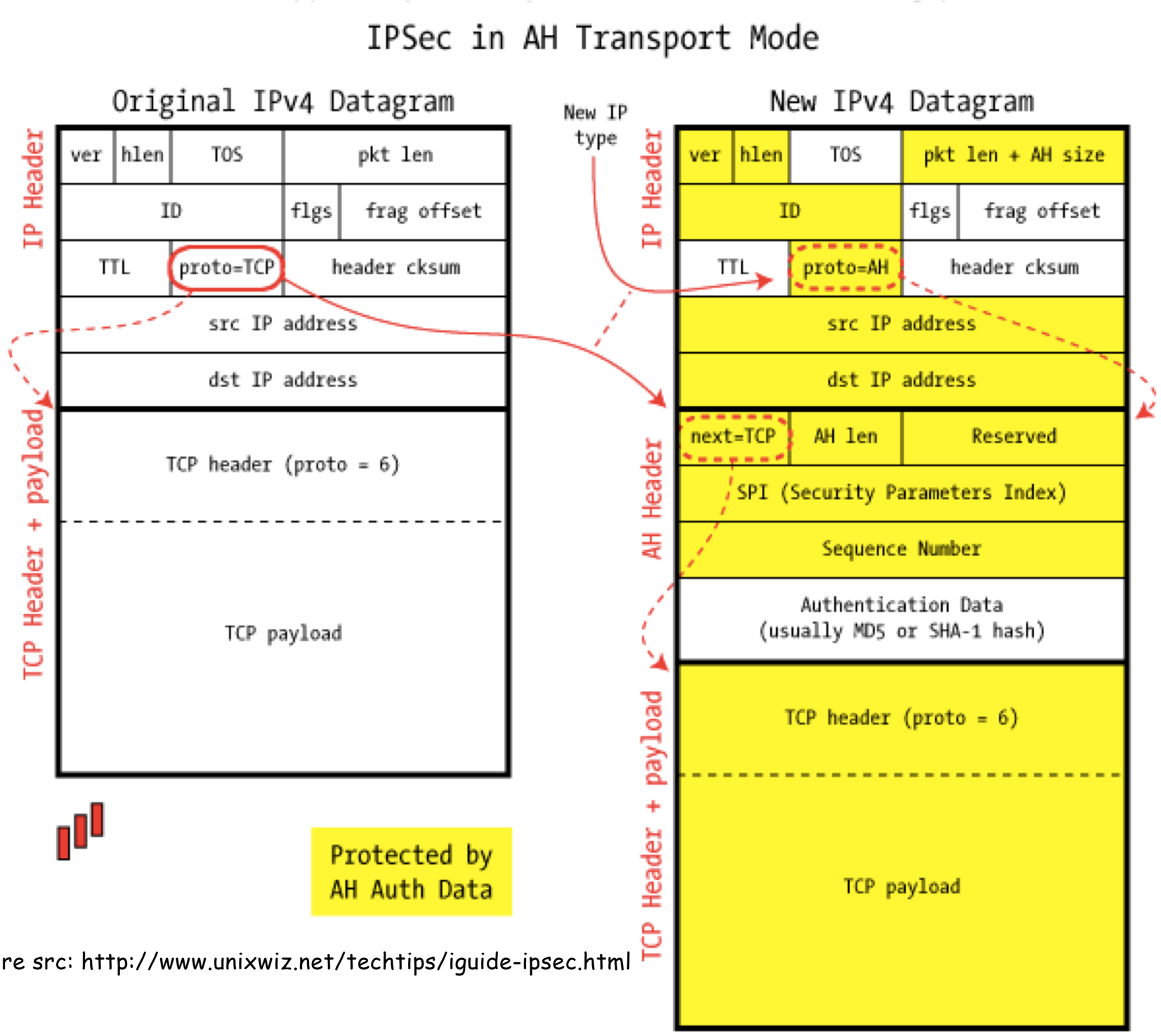


Figure src: http://www.unixwiz.net/techtips/iguide-ipsec.html

Tunnel Mode and Transport Mode Functionality (stallings Table 9.1)

No need to memorise

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

IKE Features

- Each entity has a certificate (incl. Public Key)
- Similarity with SSL handshake
  - Exchange certificates
  - Negotiate authentication and encryption algorithms
  - Securely exchange Key Material for creating session keys in the IPSec SAs

IKE phases

- IKE has two phases
  - *phase 1:* establish bi-directional IKE SA *different* from IPSec SA
    - – Authenticated and encrypted tunnel between two end points for IKE messages
    - – Est. a Master Key for use in IPSec SA in phase 2
    - – Another exchange for identity by signing their messages (Identities now protected by IKE SA, can't be sniffed)
      - » Also negotiated encryption/auth algorithms
  - *phase 2: two sides* negotiate IPSec of SA in each direction
    - No PKI in second phase, hence large number of SA negotiation possible for scalability.