Information Security
CS3002
(Sections BDS-7A/B)
Lecture 24

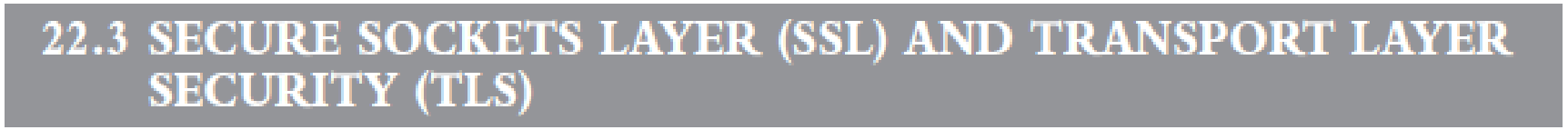
Instructor: Dr. Syed Mohammad Irteza

Assistant Professor, Department of Computer Science

13 November, 2024

Previous Lecture

- SSL, TLS
  - Maps to some parts of Chapter 22 in Computer Security: Principles and Practices (William Stallings)



Second Lecture After Mid-02 Exam

Remaining Lectures (Content)

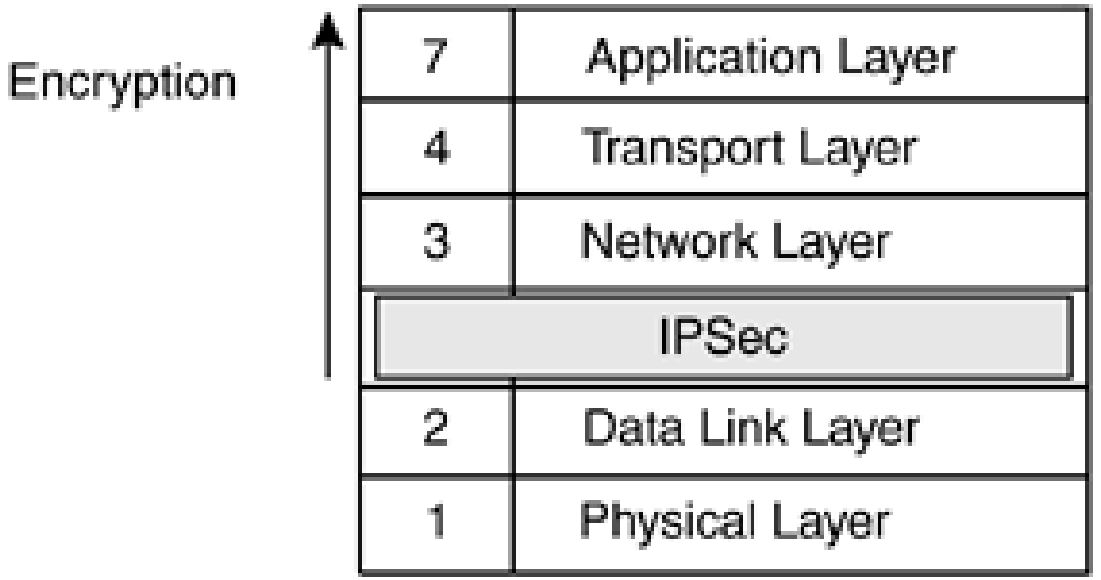
- Network Security (*3 lectures left, including this lecture*)
- Theoretical Models of Access Control (1 lecture)
- Cybercrime Laws and Ethics (1 lecture)
- Project Presentations (2 lectures at least)

Network Security – II

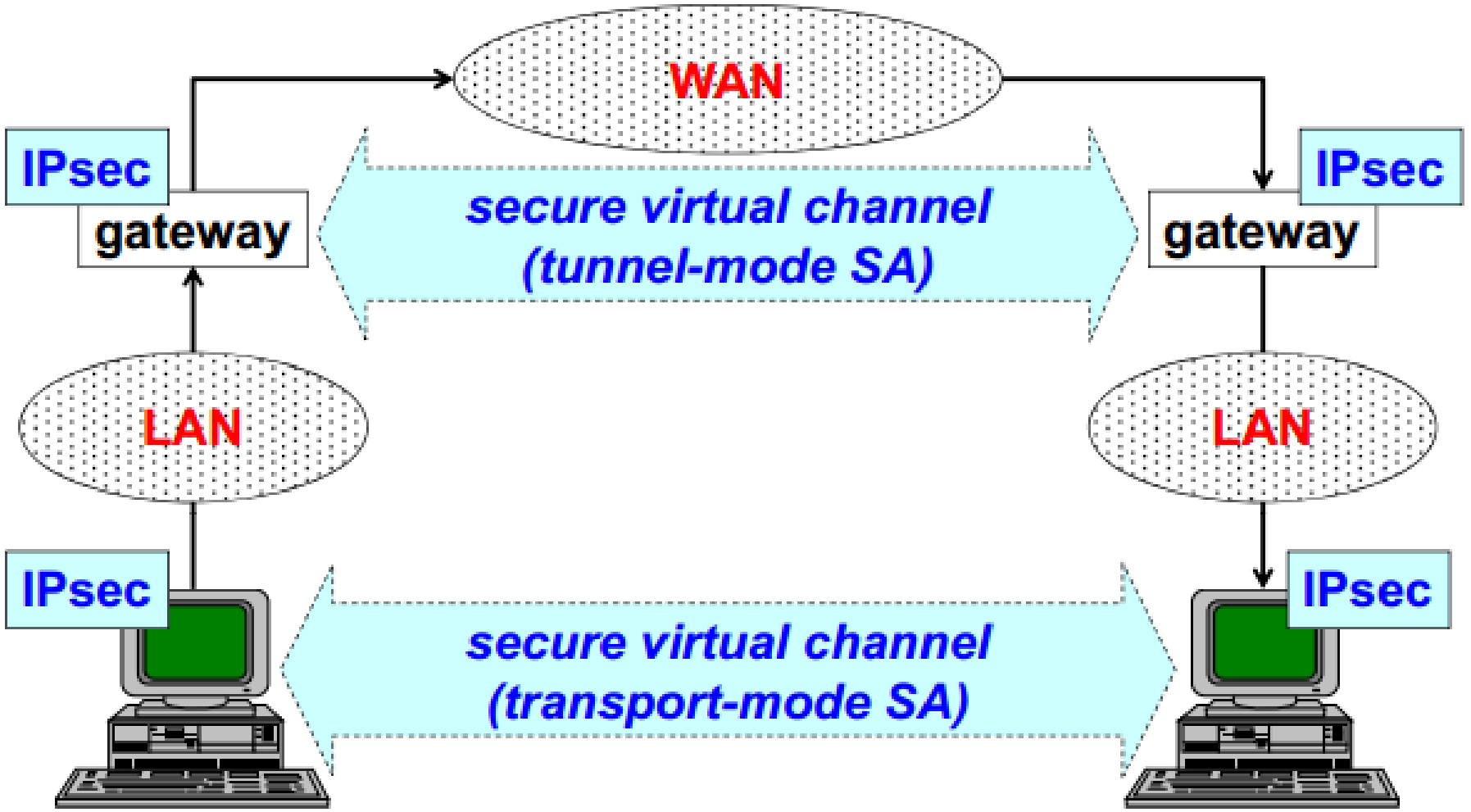
- IP Security (IPsec)
- IPsec modes
  - Transport Mode
  - Tunnel Mode
- IPsec architecture
- AH (Authentication Header)
- ESP (Encapsulation Security Payload)

IPsec

- Philosophy of IPsec: implementing ***security*** within the operating systems automatically causes applications to be protected ***without changing applications***
- IPsec is ***within the OS***. OS changes, applications and API to TCP don't.

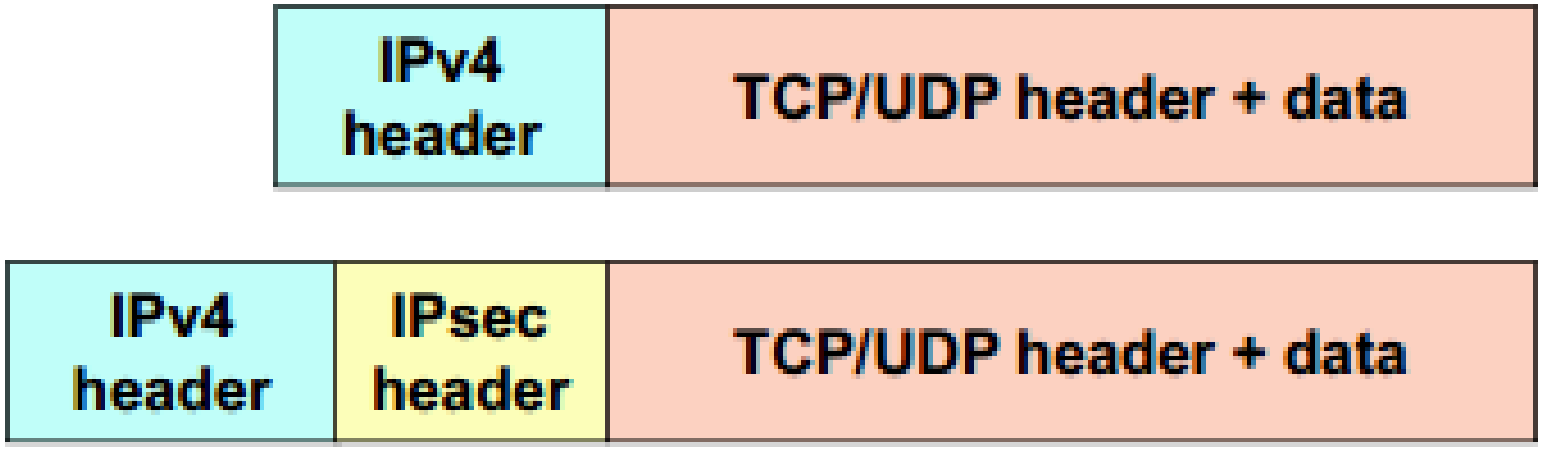


End-to-end security with basic VPN



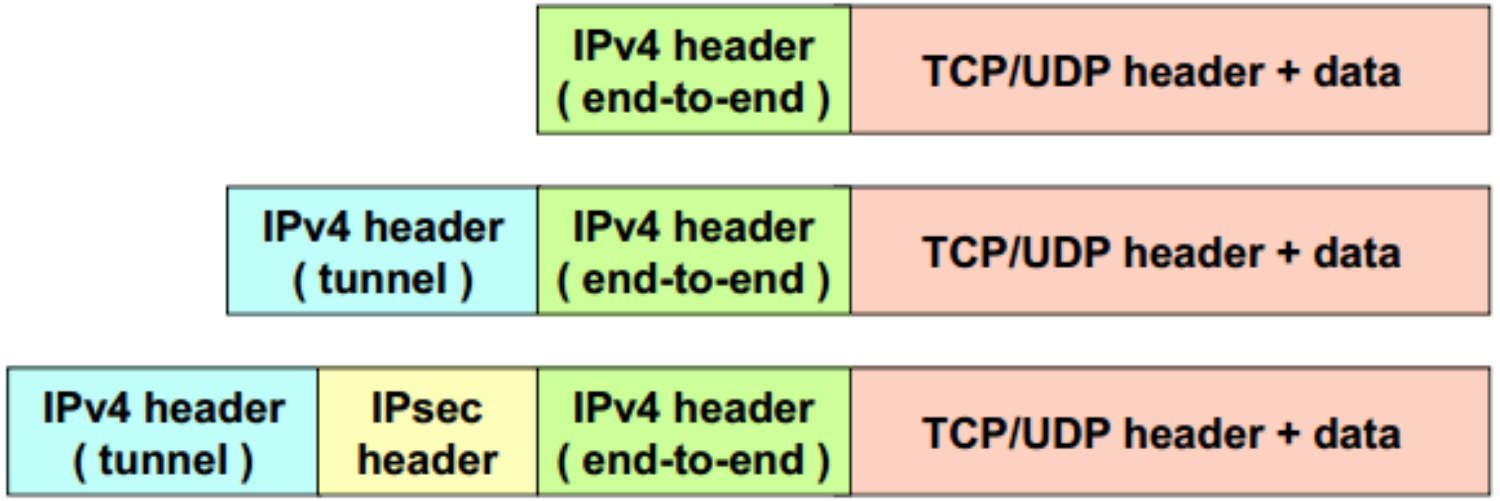
Transport mode IPsec

- Used for *end-to-end security*, that is used by *hosts*, not *gateways* (exception: traffic for the gateway itself e.g: SNMP, ICMP)
- Benefit: computationally light
- Disadvantage: no protection of header variable fields



Tunnel Mode IPsec

- used to create a *VPN*, usually by *gateways*
- Gateway-to-gateway mode
- Benefit: protection of header variable fields
- Disadvantage: computationally heavy



IPsec

- Security at layer 3 (i.e., ***network layer***)
- IPsec ensures:
  - ***Confidentiality, integrity, and authenticity (i.e., the CIA triad)***
- Allows secure communication in the Internet
- Independent from the *application* or *higher protocols*
- Network-layer security instead of application-layer security
  - Compatible with schemes providing security at the application layer
    - Can be applied simultaneously

IPsec

- Further advantages:
  - Can be applied to all network traffic
  - Routers/firewalls vendors can implement it (Can't implement SSL)
  - Transparent to the applications
  - Transparent to the users
- Limitations:
  - Limited to IP Addresses
  - Has no concept of application users

Applications of IPsec

- Secure connection among *different branches of the same company*
  - Virtual Private Network (VPN)
- Secure *remote access to an Intranet* through the (insecure) Internet
  - Allows secure remote workers
- Secure communication between peers
- Adding security for electronic commerce applications

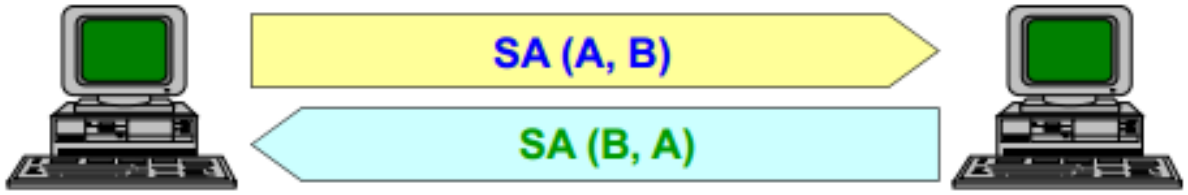
IPsec overview

IETF architecture for L3 security in IPv4 / IPv6:

- Definition of two specific packet types:
  - ***AH (Authentication Header)***
    - for integrity, authentication, no replay
  - ***ESP (Encapsulating Security Payload)***
    - for confidentiality, integrity, authentication, no replay
- Protocol for key exchange:
  - IKE (Internet Key Exchange)

Security Association

- Establishment of ***shared security attributes*** between sender and receiver to support secure communication
- Usually considered unidirectional
- Contain all the information required for execution of various network security services
- Three SA identification parameters
  - Security parameter index
  - IP destination address
  - Security protocol identifier



- Two SA are needed to get complete protection of a bidirectional packet flow in IPsec

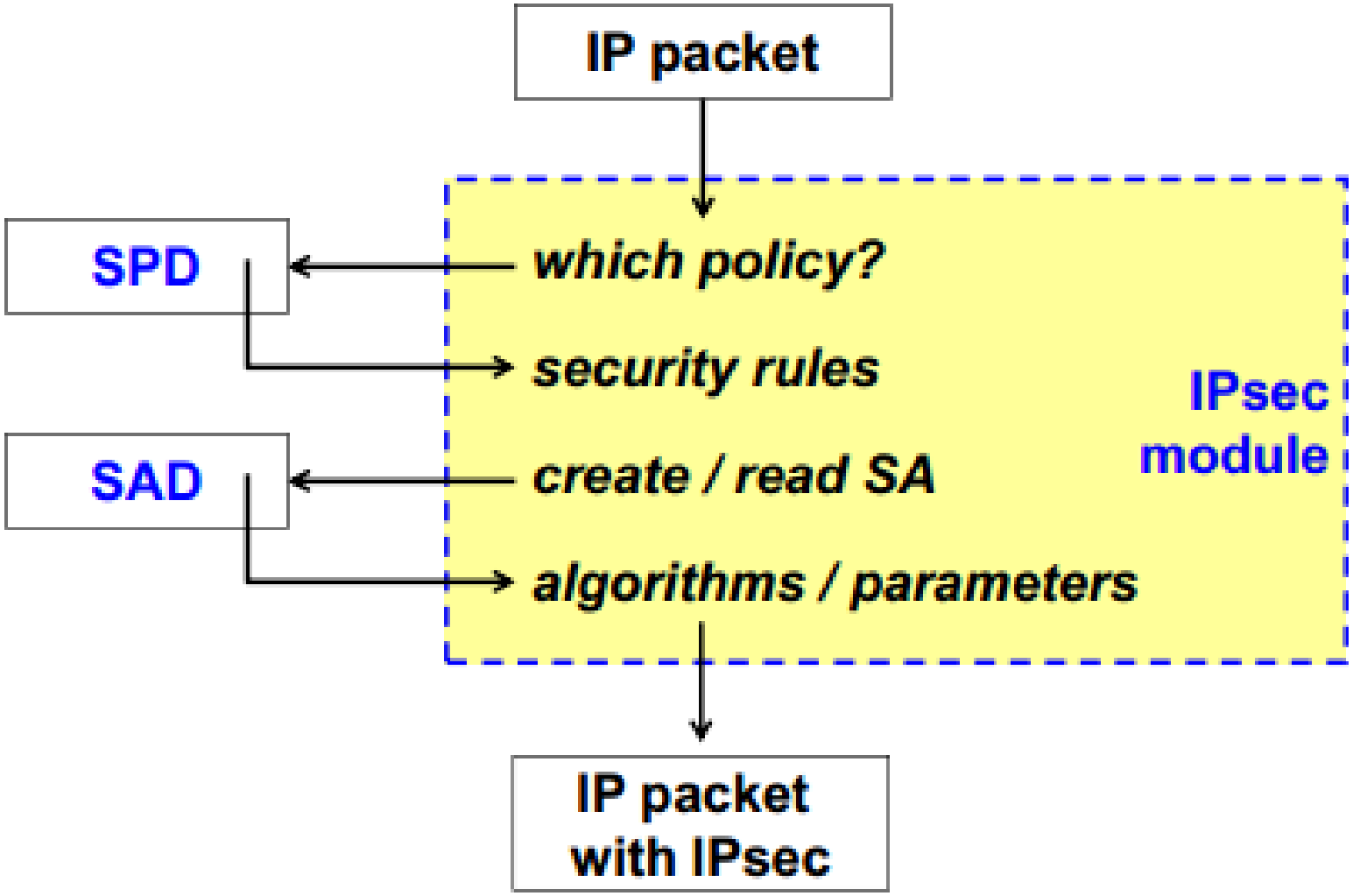
Security Association – more details

- "Security Association" is the big name for whatever a machine A needs to know in order to send IPSec-protected packets to a machine B.
- Within the memory of A is the information: "*with B, packets must use this type of IPSec header (AH or ESP) with these cryptographic algorithms and that specific key*".
- By definition, when machine A talks to machine B and uses IPSec for such communication, then there must be some convention between A and B about how this will be done.
- "Security Association" is the defined terminology to describe that convention.
- *How* a security association is established is another matter -- it can be manual configuration by sysadmins on both machines, or done dynamically with a protocol such as ISAKMP
- SPI: Uniquely identifies the SA between two parties.
- Security protocol identifier: This indicates whether the association is an AH or ESP security association.

IPsec local databases

- ***SAD (SA Database)***
  - list of active SA and their characteristics (algorithms, keys, parameters)
  - maintained by user-processes
- ***SPD (Security Policy Database)***
  - list of security policies to apply to the different packet flows
  - a-priori configured (e.g. manually) or connected to an automatic system (e.g. ISPS, Internet Security Policy System)

How IPsec works (sending)

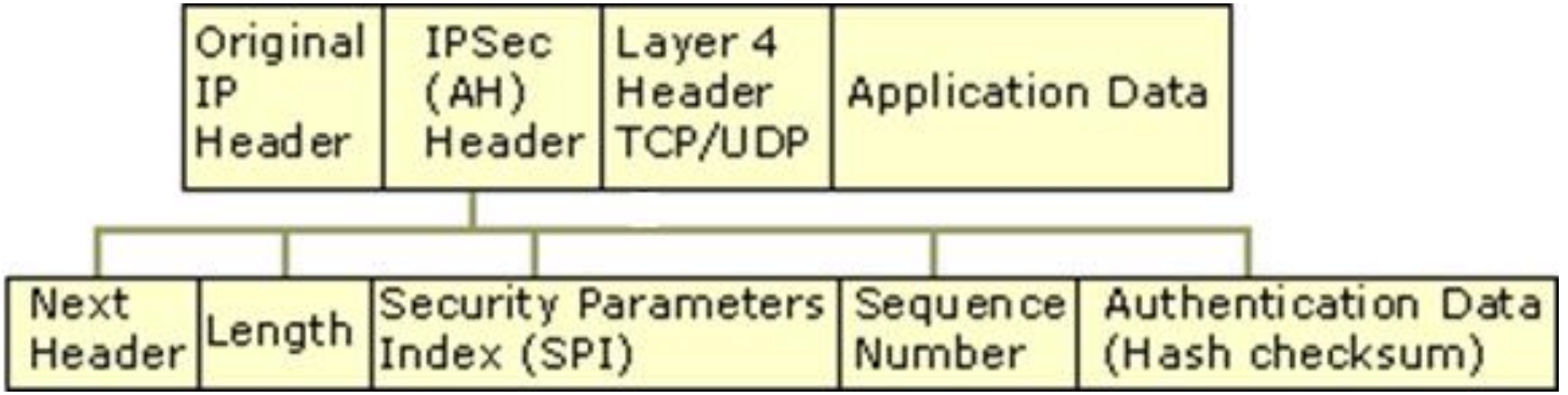


AH (Authentication Header)

- Mechanism (***first version, RFC-1826***):
  - data integrity and sender authentication
  - compulsory support of keyed-MD5 (RFC-1828)
  - optional support of keyed-SHA-1 (RFC-1852)

- Mechanism (***second version, RFC-2402)***:
  - data integrity, sender authentication and protection from replay attack
  - HMAC-MD5
  - HMAC-SHA-1

AH Packet



- Next header: identifies the nature of the payload (TCP/UDP)
- Length: Indicates the length of the AH header
- SPI: Identifies the correct security association for the communication
- Sequence Number: Provides anti-replay protection for the SA
- Auth. Data: contains the Integrity Check Value (ICV) that is used to verify the integrity of the message. The receiver calculates the hash value and checks it against this value (calculated by the sender) to verify integrity.

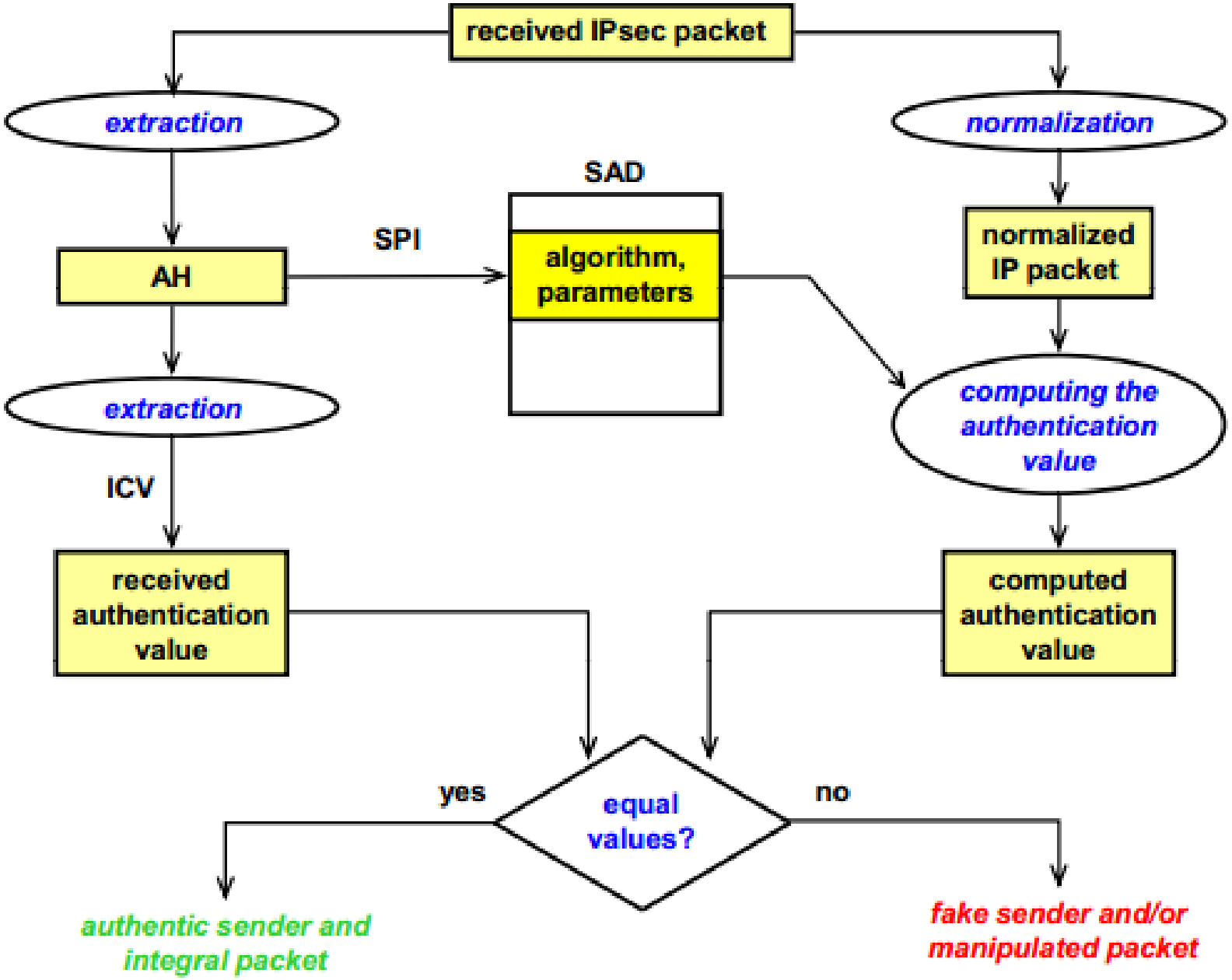
AH verification

Traffic normalizer: normalizes traffic in such a way that Network Intrusion Detection Systems (NIDS) are able to avoid penetrations by attackers by exploiting the ambiguities in the traffic stream as seen by the monitor.

E.g: packet maybe fragmented by the attacker so that its reassembled at the user end by evading through the NIDS.

https://users.ece.cmu.edu/~vsekar/Teaching/Spring18/18731/reading/NIDS_Handley.pdf

Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics Mark Handley and Vern Paxson



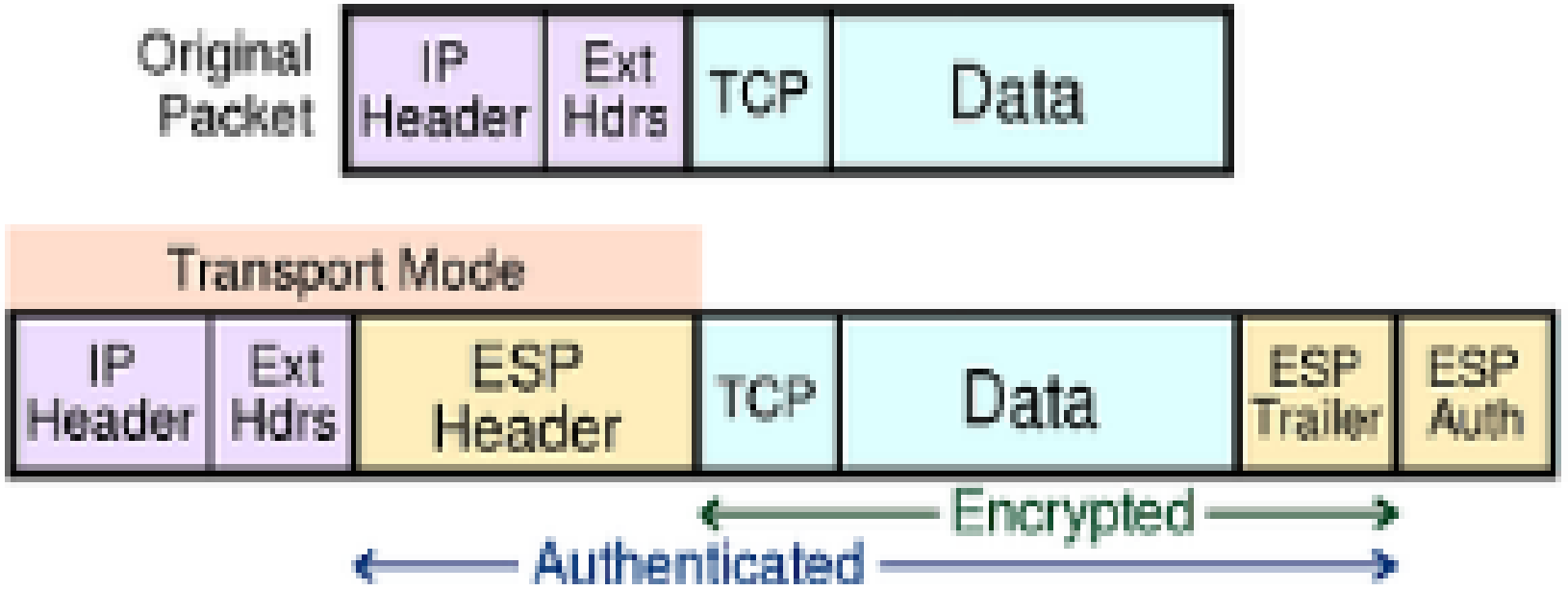
ESP (Encapsulating Security Payload)

- ***First version (RFC-1827)*** gave only confidentiality
  - base mechanism: DES-CBC (RFC-1829)

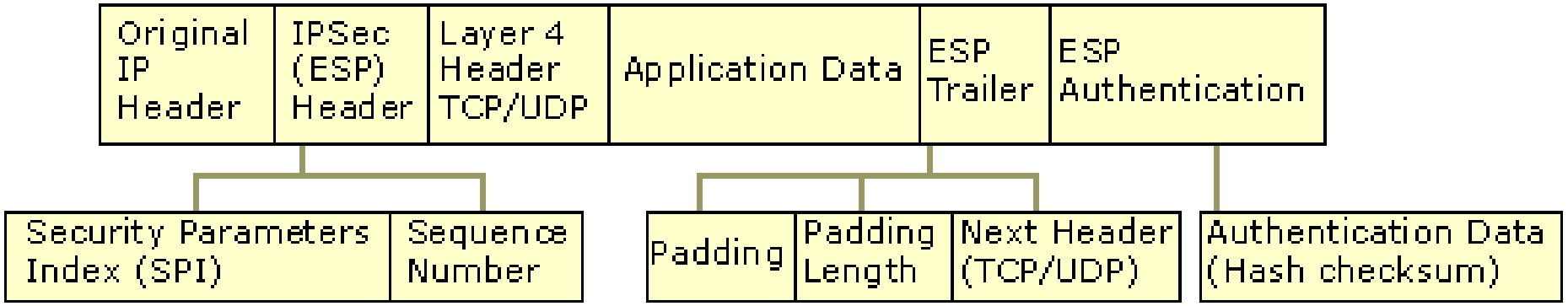
- ***Second version (RFC-2406)***:
  - provides confidentiality & authentication (but not the IP header, so the coverage is not equivalent to that of AH)

ESP in transport mode

- Benefit: the payload is hidden (including info needed for QoS or intrusion detection)
- Disadvantage: the header remains in clear

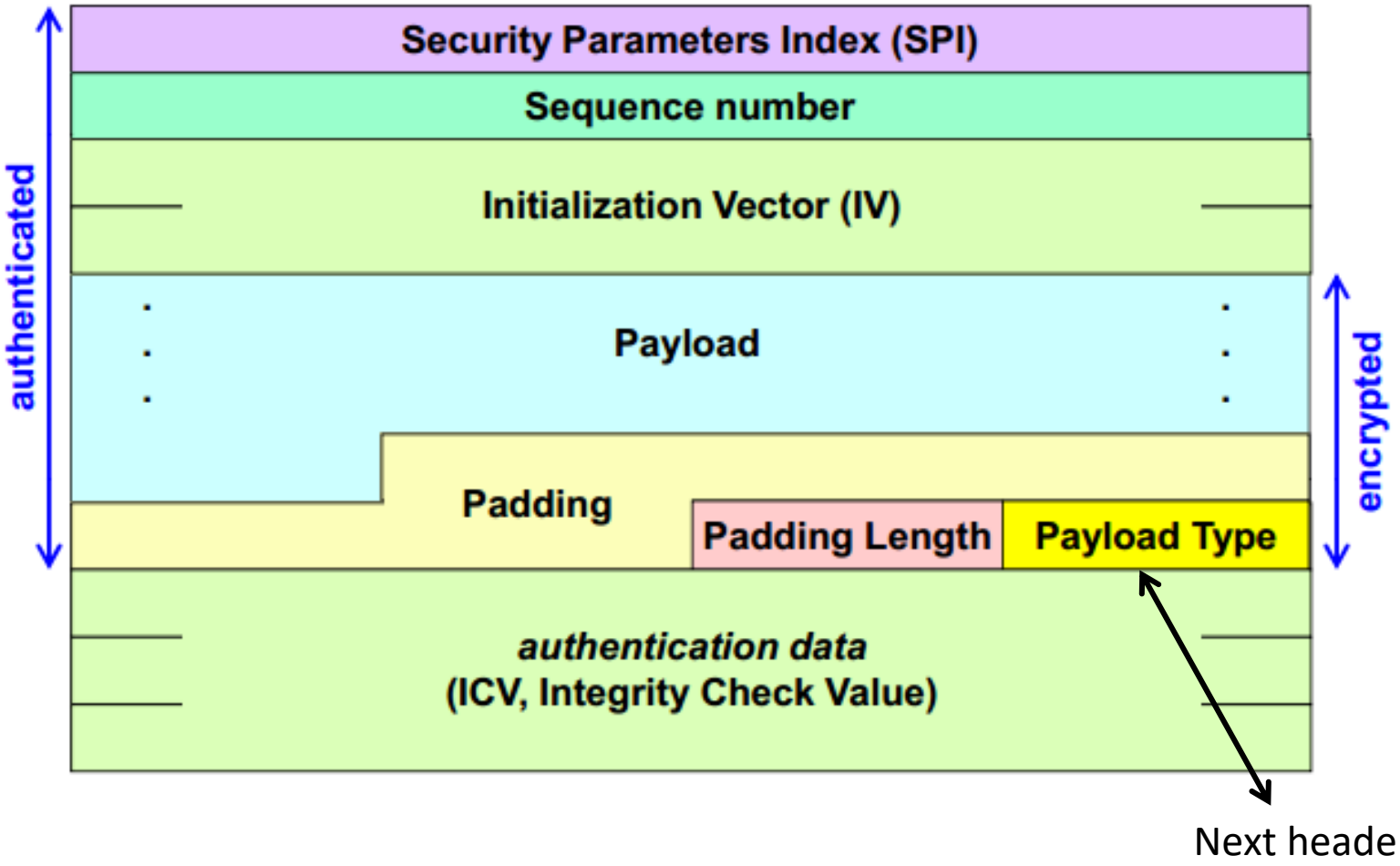


ESP Packet



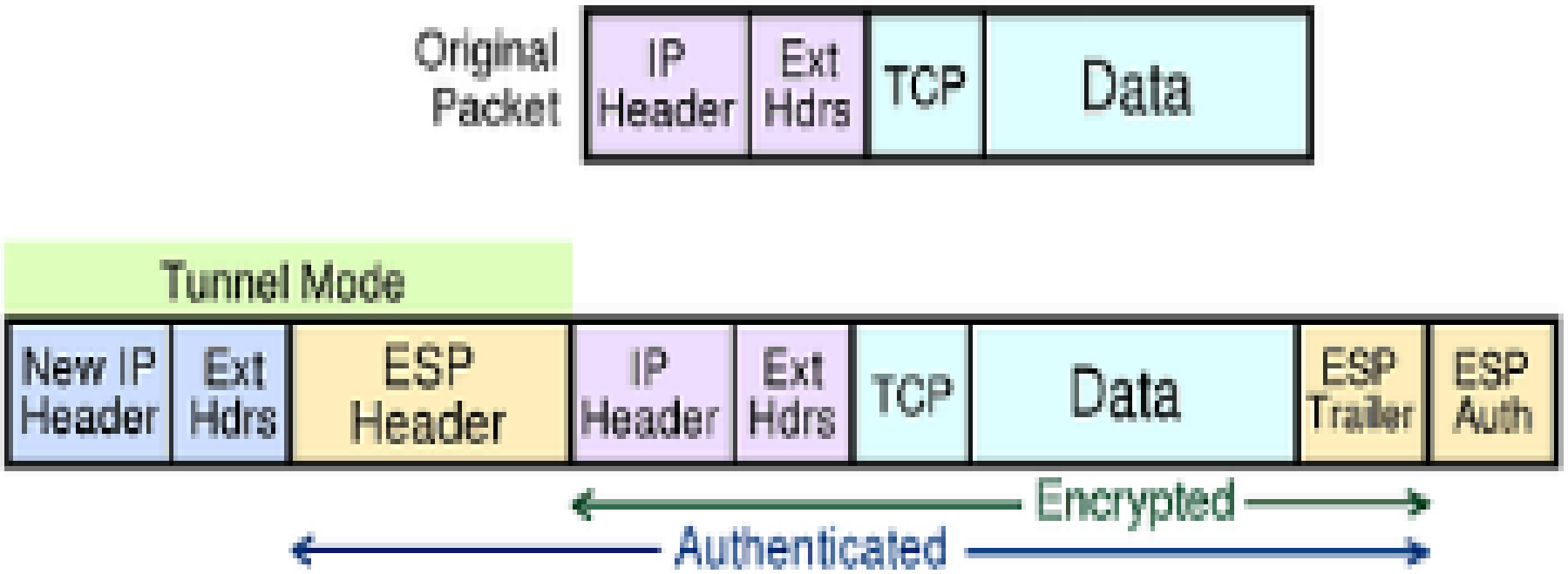
- SPI: Identifies the correct security association for the communication
- Sequence number: Provides anti-replay protection for the SA
- Next header: Identifies the nature of the payload (TCP/UDP)
- Auth. Data: Contains the Integrity Check Value (ICV), and a message authentication code that is used to verify the sender's identity and message integrity. The ICV is calculated over the ESP header, the payload data and the ESP trailer
- Initialization Vector (IV): optional. Is after the Sequence number

ESP Packet: Encryption & Authentication

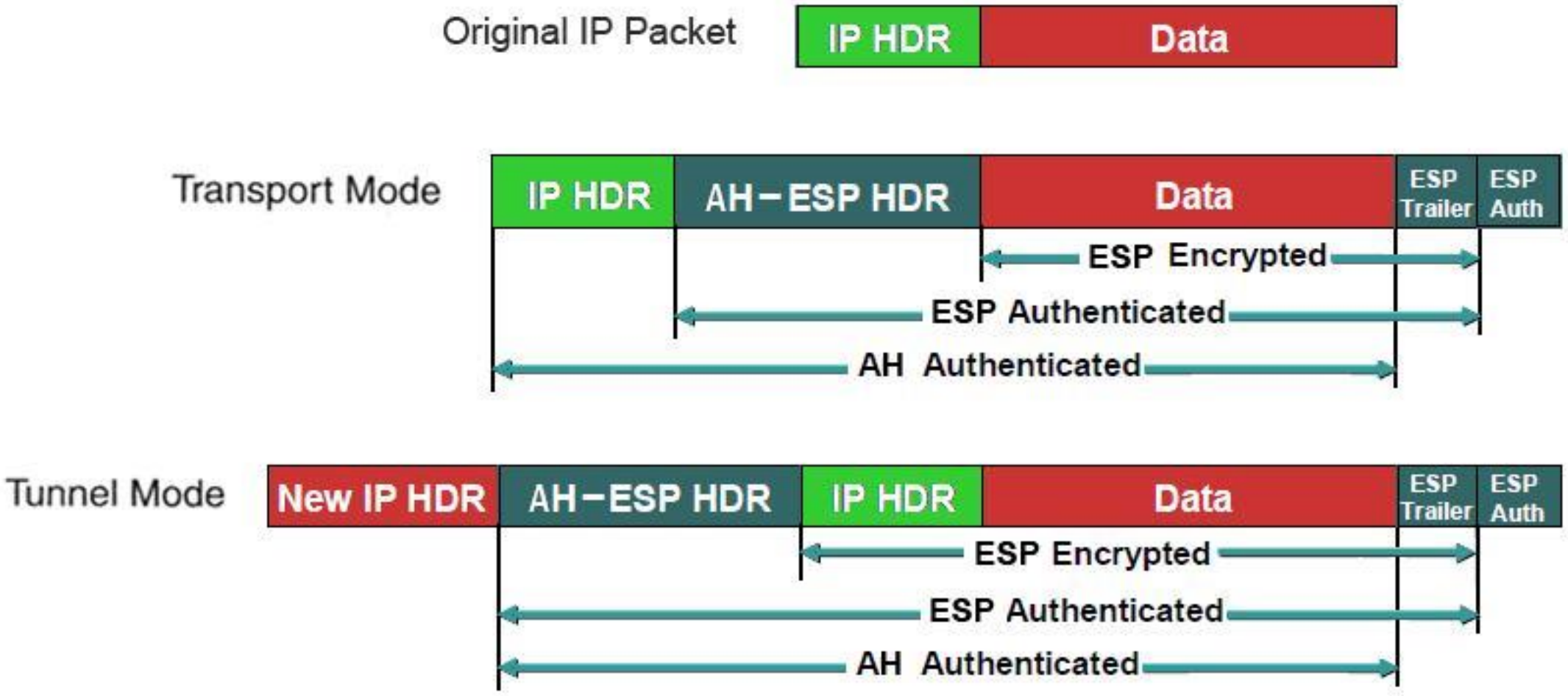


ESP tunnel mode

- Benefit: hides both the payload and (original) header
- Disadvantage: larger packet size



IPSec: AH & ESP packet format



Appendix

- What is IPSec? – YouTube (Palo Alto Networks)

Acknowledgments

- Dr Haroon Mahmood and other FAST-NU instructors