IPsec

IPsec

- A Network Layer protocol suite for providing security over IP.
- Part of IPv6; an add-on for IPv4.
- Can handle all three possible security architectures:

Feature	Gateway-to-Gateway	Host-to-Gateway	Host-to-Host
Protection between client and local gateway	No	N/A (client is VPN endpoint)	N/A (client is VPN endpoint)
Protection between VPN endpoints	Yes	Yes	Yes
Protection between remote gateway and remote server (behind gateway)	No	No	N/A (client is VPN endpoint)
Transparency to users	Yes	No	No
Transparency to users' systems	Yes	No	No
Transparency to servers	Yes	Yes	No

IPsec services

- Basic functions, provided by separate (sub-)protocols:
  - Authentication Header (AH): Support for data integrity and authentication of IP packets.
  - Encapsulated Security Payload (ESP): Support for encryption and (optionally) authentication.
  - Internet Key Exchange (IKE): Support for key management etc.

Service	AH	ESP (encrypt only)	ESP(encrypt+authent.)
Access Control	+	+	+
Connectionless integrity	+		+
Protection between VPN endpoints	+		+
Data origin authentication	+		+
Reject replayed packets		+	+
Payload confidentiality		+	+
Metadata confidentiality		partial	partial
Traffic flow confidentiality		(*)	(*)

IPsec Security Associations

- Think of it as an IPsec connection: all of the parameters needed, like crypto algorithms (AES, SHA1, etc.), modes of operation (CBC, HMAC, etc.), key lengths, traffic to be protected, etc.
- Both sides must agree on the SA for secure communications to work
- For a two-way communication, two SAs must be defined.
- SA parameters must be negotiated (using IKE) between sender and receiver before secure communication can start.
- Each SA is identified by:
  - Security Parameters Index (SPI): 32-bit integer chosen by sender. Enables receiving system to select the required SA.
  - Destination Address: Only unicast IP addresses allowed!
  - Security Protocol Identifier: AH or ESP.

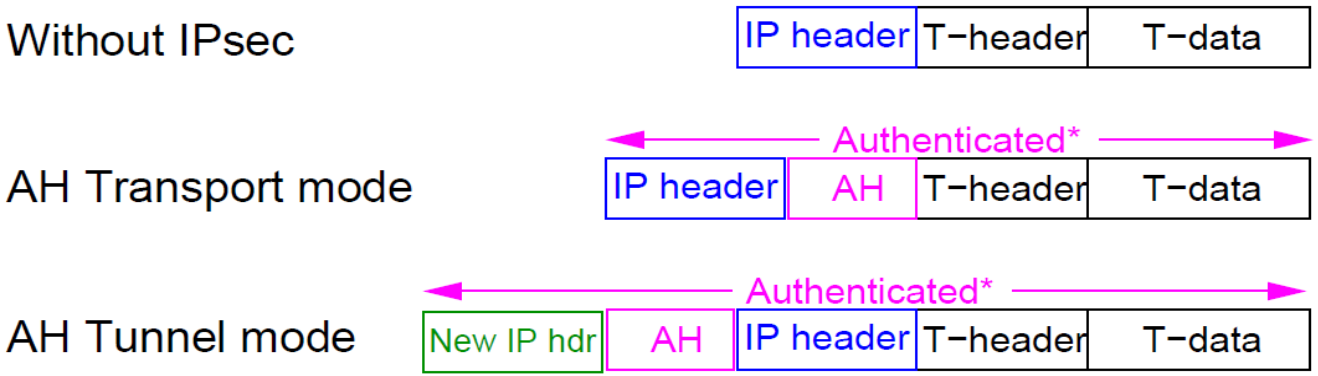
IPsec modes

- Transport Mode
  - Provides protection for a T-layer packet embedded as payload in an IP packet.
- Tunnel Mode
  - Provides protection for an IP packet embedded as payload in an IP packet.

	Transport Mode SA	Tunnel Mode SA
AH	Authenticate IP payload and selected parts of IP header and IPv6 extension headers.	Authenticate entire inner IP packet and selected parts of outer IP header and outer IPv6 extension headers.
ESP	Encrypt IP payload + any IPv6 extension headers after ESP header.	Encrypt inner IP packet.
ESP + authent.	Encrypt IP payload + any IPv6 extension headers after ESP header. Authenticate IP payload.	Encrypt and authenticate inner IP packet.

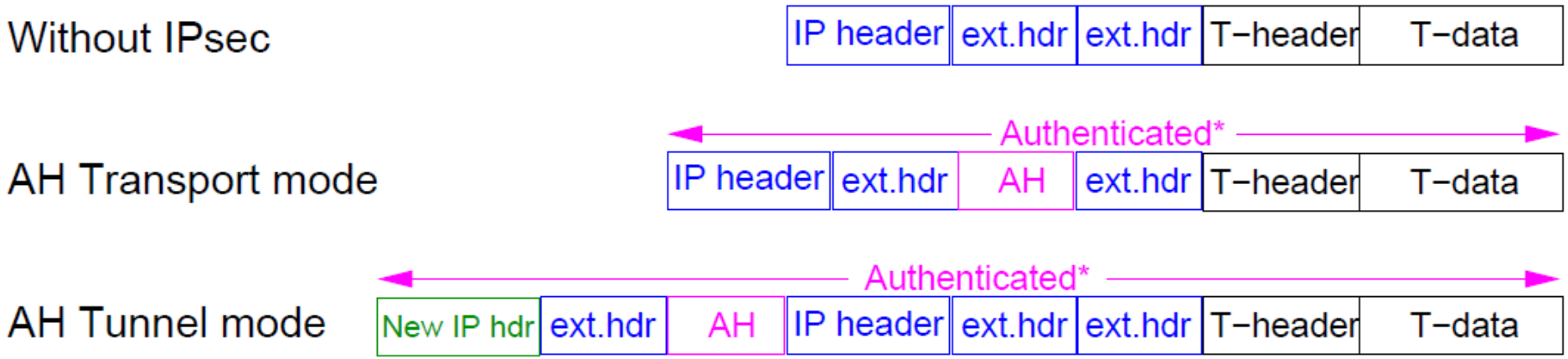
Authentication with IPv4

- AH header inserted after the outermost IP header – depending on whether Transport or Tunnel mode is used.
  - Do not forget that integrity check (and thus authentication) does not cover any mutable, unpredictable header fields.



Authentication with IPv6

- AH header inserted after the outermost IP header – depending on whether Transport or Tunnel mode is used.
  - Do not forget that integrity check (and thus authentication) does not cover any mutable, unpredictable header fields.

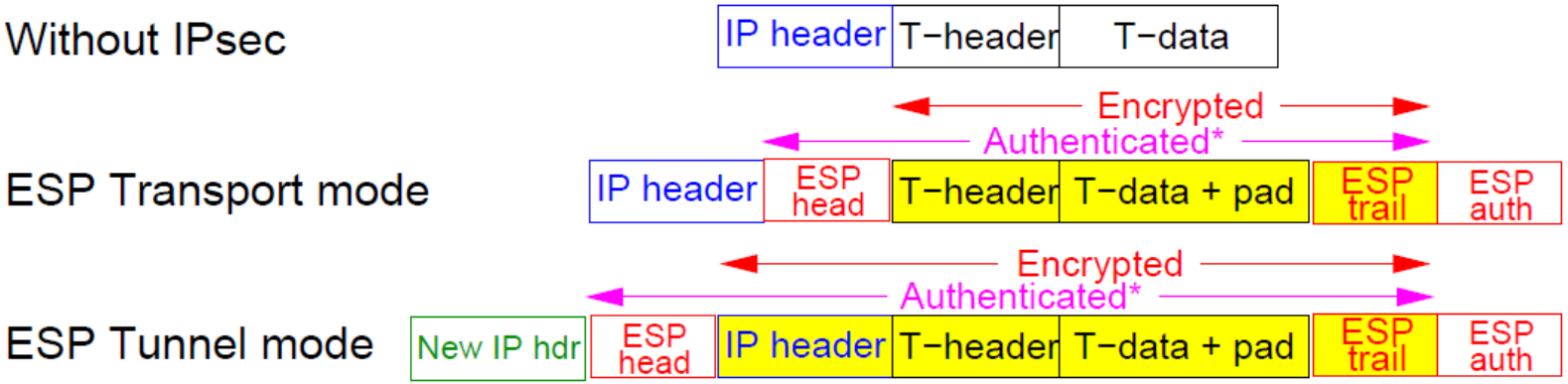


Authentication Header

- One of the (many possible) IP header fields. Contains:
  - Next Header: Type of following header field.
  - Payload Length: (Length - 2), in 32-bit words, of AH.
  - SPI: Identifies SA in use.
  - Sequence Number: Monotonically increasing packet counter value.
  - Authentication Data (AD): (variable length) HMAC based on MD5 or SHA-1 criptorgraphic hashing algorithm, or AES-CBC, evaluated over:
    - Immutable or predictable IP header fields. (Other fields assumed zero when MAC is calculated.)
    - Rest of AH header apart from AD field.
    - All embedded payload (from T-layer or embedded IP packet), assumed immutable.
- Immutable fields do not change as the packet traverses the network.
  - Example: Source address.
- Mutable but predictable fields may change, but can be predicted.
  - Example: Destination address.
- Mutable, unpredictable fields include Time-to-live, Header checksum.

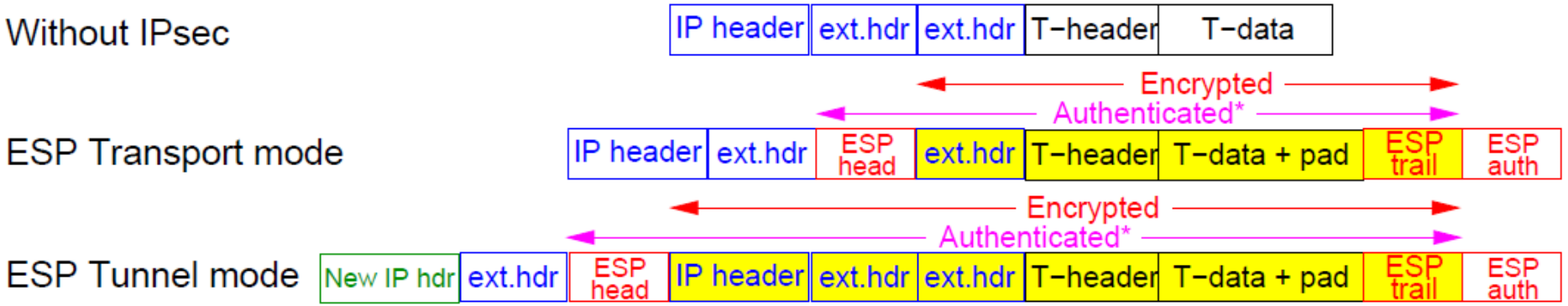
ESP with IPv4

- ESP header inserted after the outermost IP header – depending on whether Transport or Tunnel mode is used:
  - Padding is added to end of T-layer payload to give (a certain amount) of traffic analysis protection.
  - ESP trailer and (optional) ESP authentication field added after the end of the padded T-layer payload.
- As usual, authentication/integrity does not cover any mutable, unpredictable header fields.



ESP with IPv6

- ESP header inserted after the outermost IP header – depending on whether Transport or Tunnel mode is used:
  - Padding is added to end of T-layer payload to give (a certain amount) of traffic analysis protection.
  - ESP trailer and (optional) ESP authentication field added after the end of the padded T-layer payload.
- As usual, authentication/integrity does not cover any mutable, unpredictable header fields.



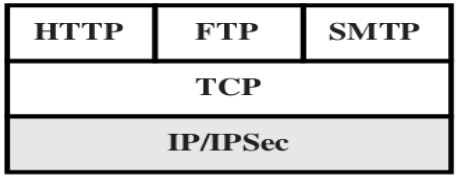
Encryption + Authentication

A common combination, can be achieved by:

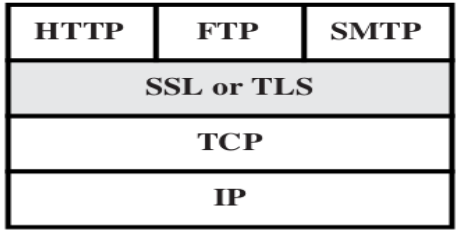
1) ESP with Authentication. First apply ESP to data, then add AH field. Two subcases:
    1) Transport mode: E+A apply to IP payload, but IP header not protected.
    2) Tunnel mode: E+A apply to entire inner packet.
2) Transport Adjacency. Use bundled SAs, first ESP, then AH.
3) Encryption covers original IP payload. Authentication covers ESP + original IP header, including source and destination IP addresses
4) Transport-Tunnel bundle. Used to achieve authentication before encryption, for example via inner AH transport SA and outer ESP tunnel SA.
5) Authentication covers IP payload + IP immutable header. Encryption is applied to entire authenticated inner packet.

IPsec vs TLS

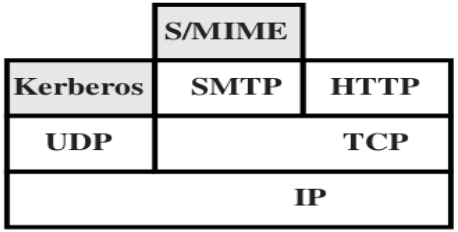
- TLS much more flexible because is in the upper levels
- TLS also provides application end-to-end security, best for web applications → HTTPS
- IPsec hast to run in kernel space
- IPsec much more complex and complicated to manage with



(a) Network level



(b) Transport level



(c) Application level

That's all for today

- **Questions?**
- Resources:
  - Chapter 24 textbook
  - "Virtual private networking", Gilbert Held, Wiley ed.
  - http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm
  - "Guide to IPsec VPNs", NIST800-77
  - "Guide to SSL VPNs", NIST-SP800-113