Network Security

AA 2020/2021

Security Protocols

Examples

- IPSec
- WLAN Security
- DNS

Typical Attacks to IPv4

- Lack of confidentiality (stealing credentials)
- Lack of source authentication (spoofing, DOS)
- Source routing (spoofing and redirection)

IP Security Objectives

- Application level:
  - Transparent to applications and users (below transport layer)
- Host Level
  - Provide security for individual hosts
- Router Level
  - router or neighbor advertisements come from authorized routers
  - redirect message come from routers to which the initial packet was sent
  - A routing update is not forged

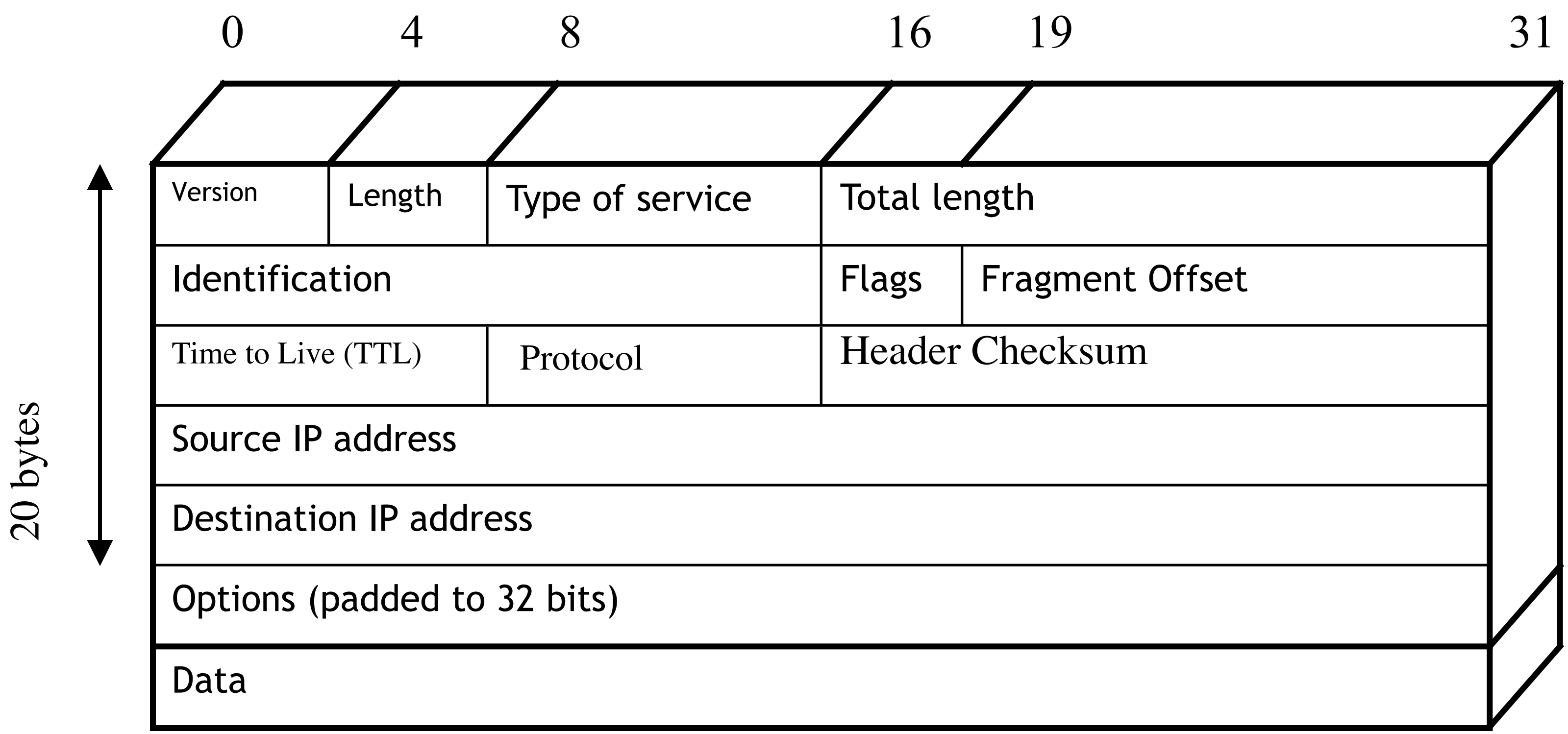
IPSec

- A set of security protocols
- A general framework that allows a pair of communicating entities (IP addresses!) to choose the appropriate crypto for the communication.
- IPSec service
    - Connectionless integrity
    - Data origin authentication
    - Rejection of replayed packets
    - Confidentiality (encryption)
    - Limited traffic flow confidentiallity

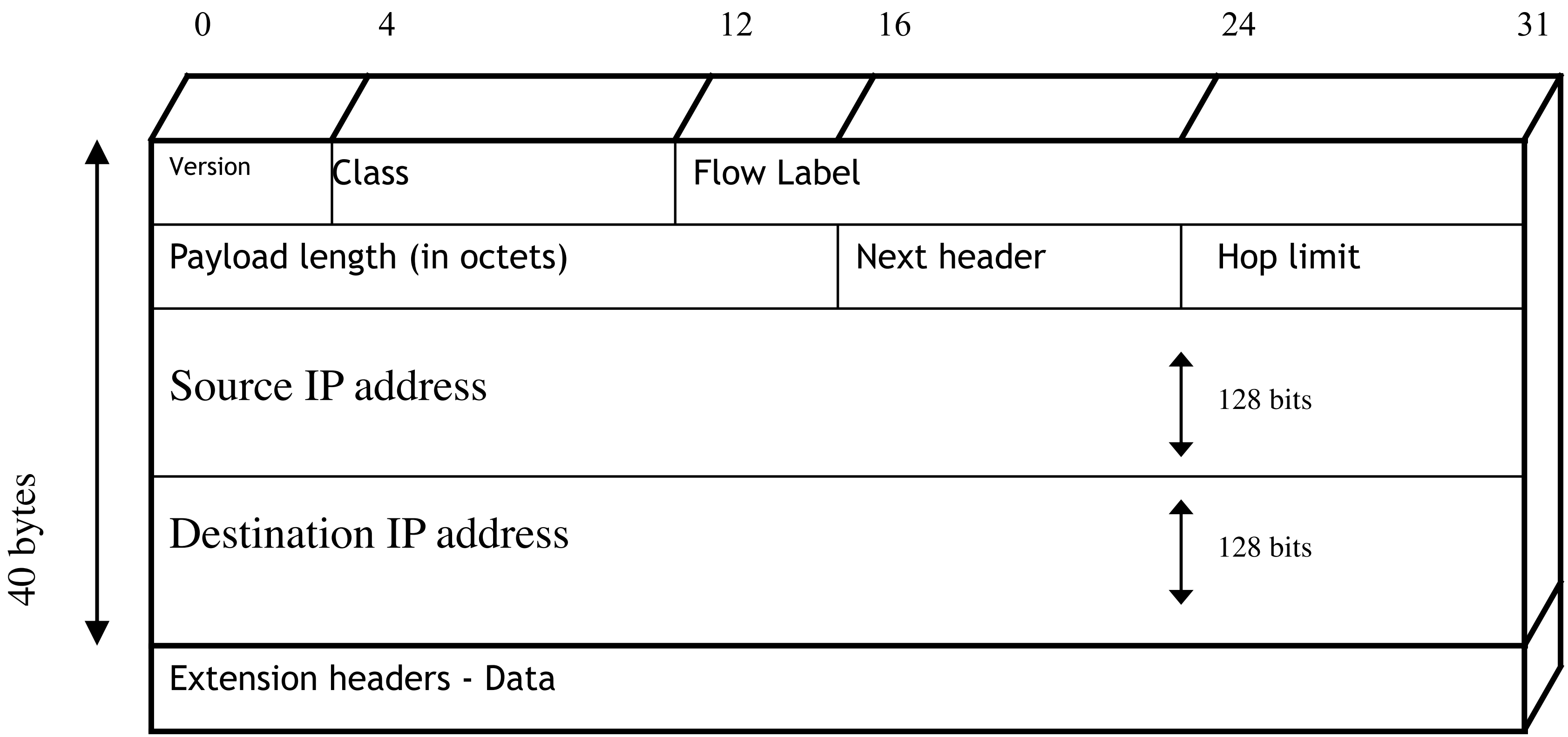
IPsec Basic Features

- Two basic modes of use:
  - “Transport” mode: for IPsec-aware hosts as endpoints.
  - “Tunnel” mode: for IPsec-unaware hosts, established by intermediate gateways or host OS.
- Provides authentication and/or confidentiality services for data.
  - AH and ESP protocols.
- Provides flexible set of key establishment methods:
  - IKE, IKEv2.

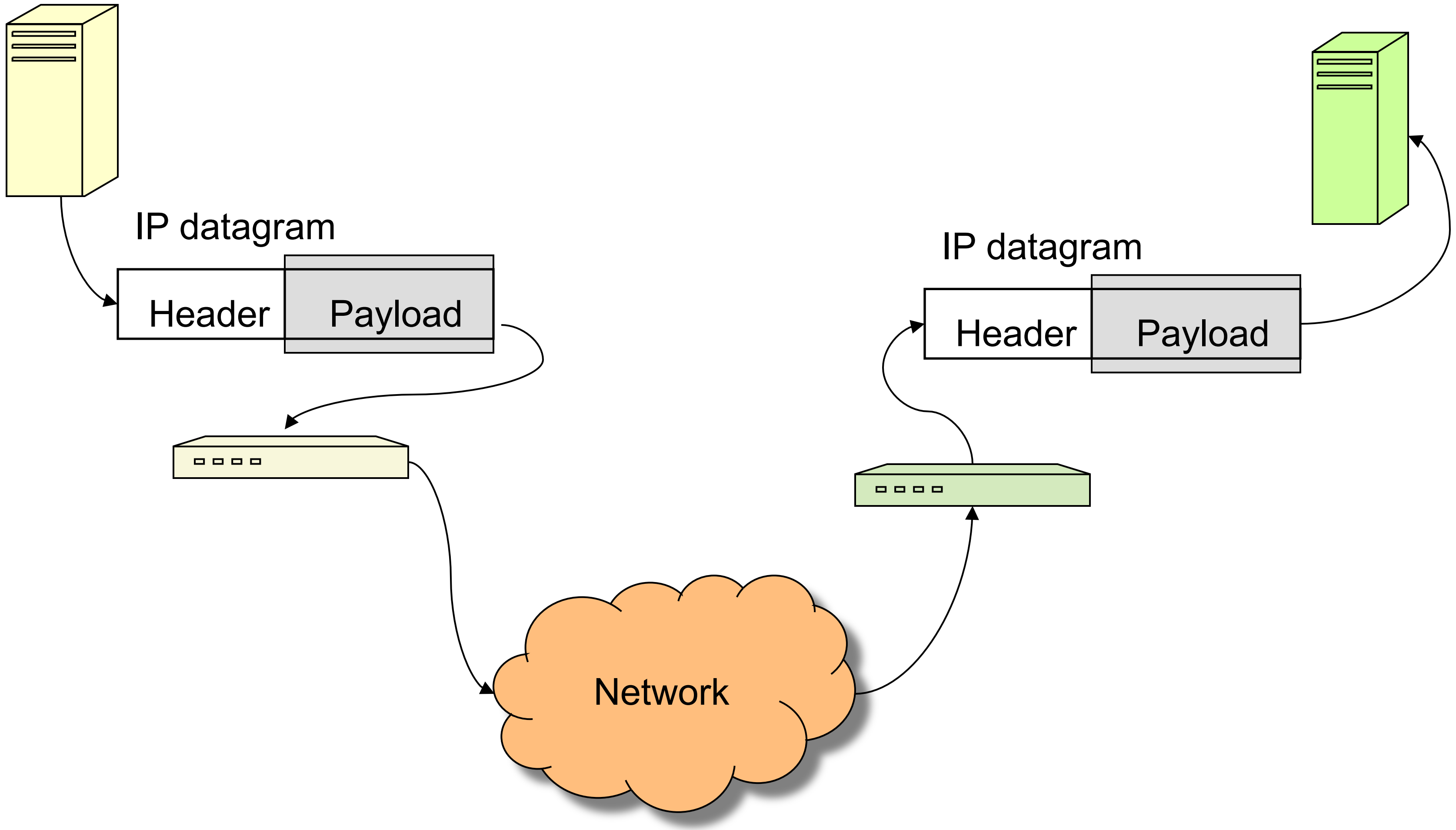
IPv4 Header


0
4
8
16
19
31
Version
Length
Type of service
Total length
Identification
Flags
Fragment Offset
Time to Live (TTL)
Protocol
Header Checksum
Source IP address
Destination IP address
Options (padded to 32 bits)
Data
20 bytes

IPv6 Header


0
4
12
16
24
31
Version
Class
Flow Label
Payload length (in octets)
Next header
Hop limit
Source IP address
128 bits
Destination IP address
128 bits
Extension headers - Data
40 bytes

IPSec Transport Mode

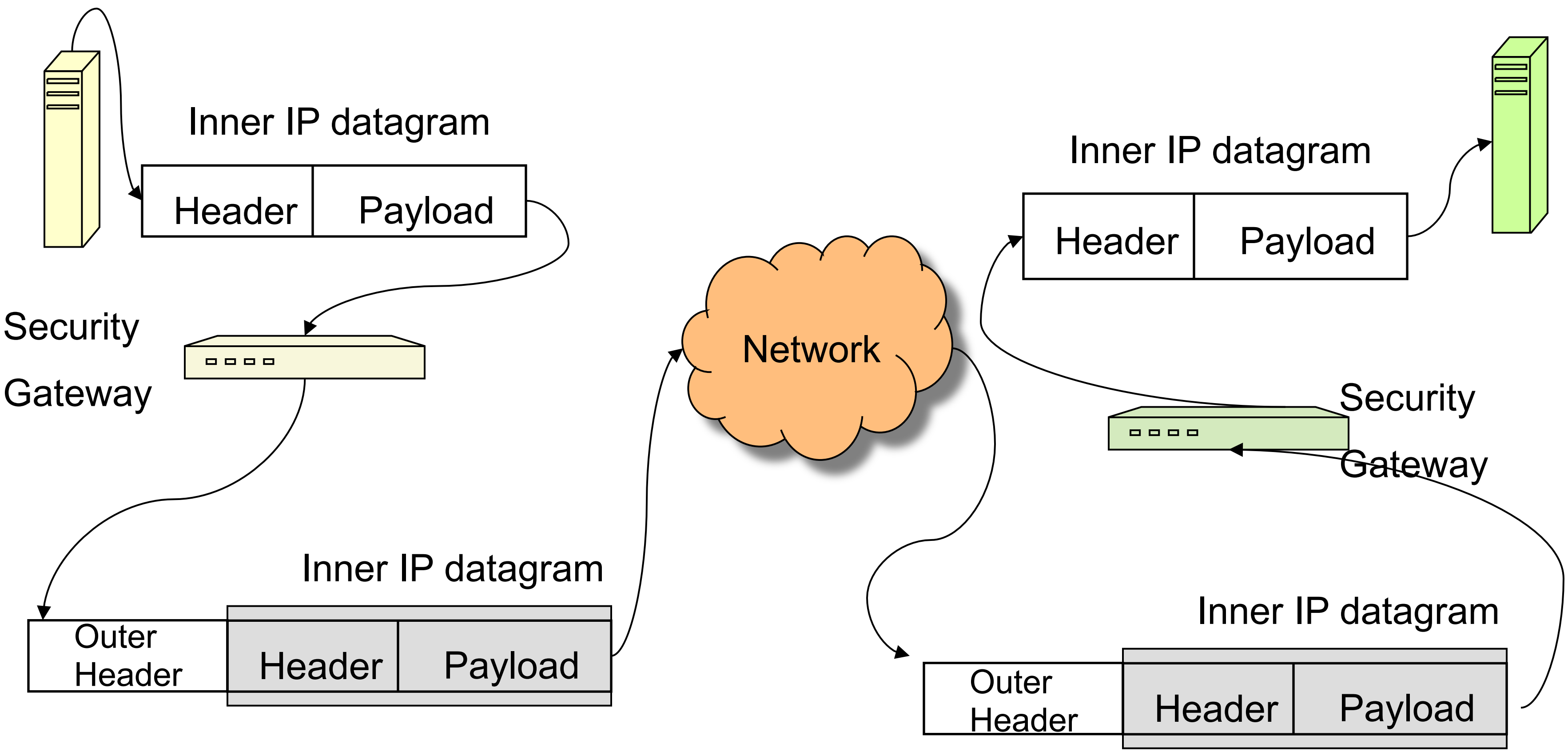


IPsec Transport Mode

- Protection for upper-layer protocols.
- Protection covers IP datagram payload (and selected header fields).
  - Could be TCP packet, UDP, ICMP message,….
- Host-to-host (end-to-end) security:
  - IPsec processing performed at endpoints of secure channel.
  - Endpoint hosts must be IPsec-aware.

UNIVERSITÀ DEGLI STUDI DI TRENTO

IPsec Tunnel Mode



IPsec Tunnel Mode

- Protection for entire IP datagram.
- Entire datagram plus security fields treated as new payload of ‘outer’ IP datagram.
- Original ‘inner’ IP datagram encapsulated within ‘outer’ IP datagram.
- IPsec processing performed at security gateways on behalf of endpoint hosts.
  - Gateway could be perimeter firewall or router.
  - Gateway-to-gateway rather than end-to-end security.
  - Hosts need not be IPsec-aware.
- Inner IP datagram not visible to intermediate routers:
  - Even original source and destination addresses encapsulated and so ‘hidden’.

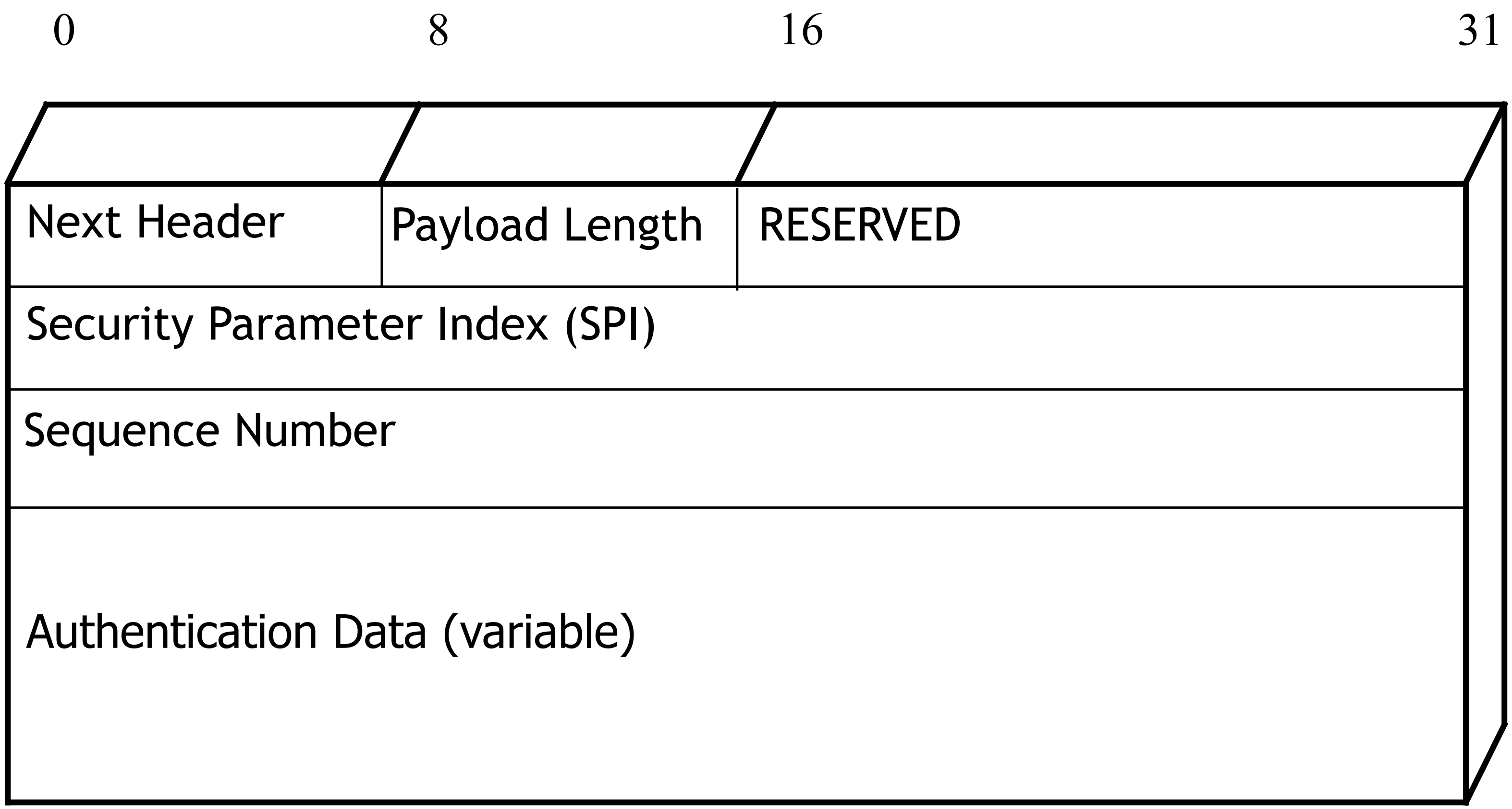
Protocols

- AH: Authentication Header for authentication and integrity
- ESP: Encapsulating Security Payload for confidentiality and authentication

AH Protocol

- AH = Authentication Header (RFC 2402).
- Provides data origin authentication and data integrity.
- AH authenticates whole payload and most of header.
- Prevents IP address spoofing.
  - Source IP address is authenticated.
- Creates stateful channel.
  - Use of sequence numbers.
- Prevents replay of old datagrams.
  - AH sequence number is authenticated.
- Uses MAC and secret key shared between endpoints.

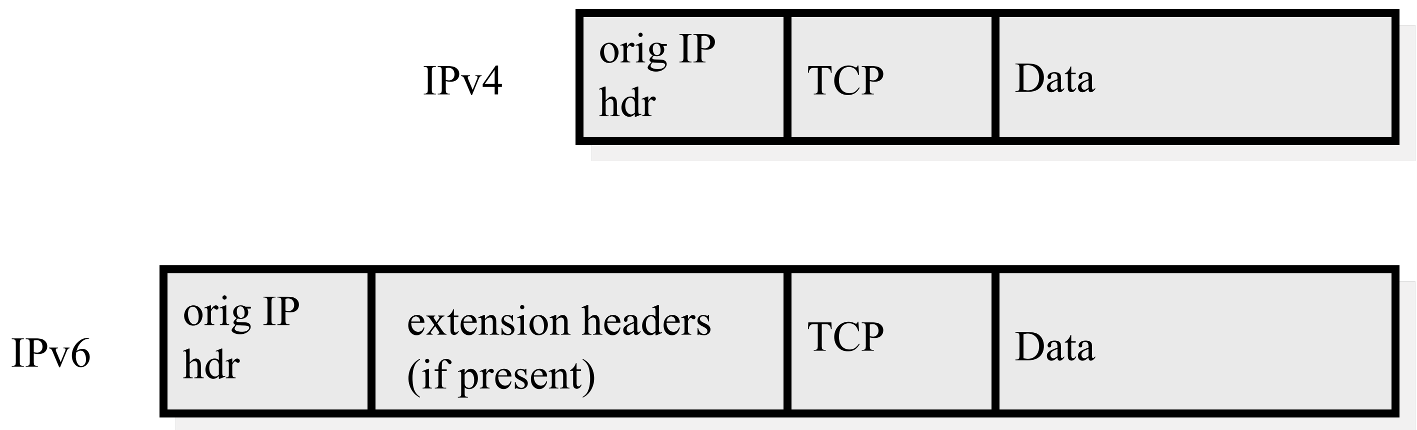
Authentication Header (RFC 2402)



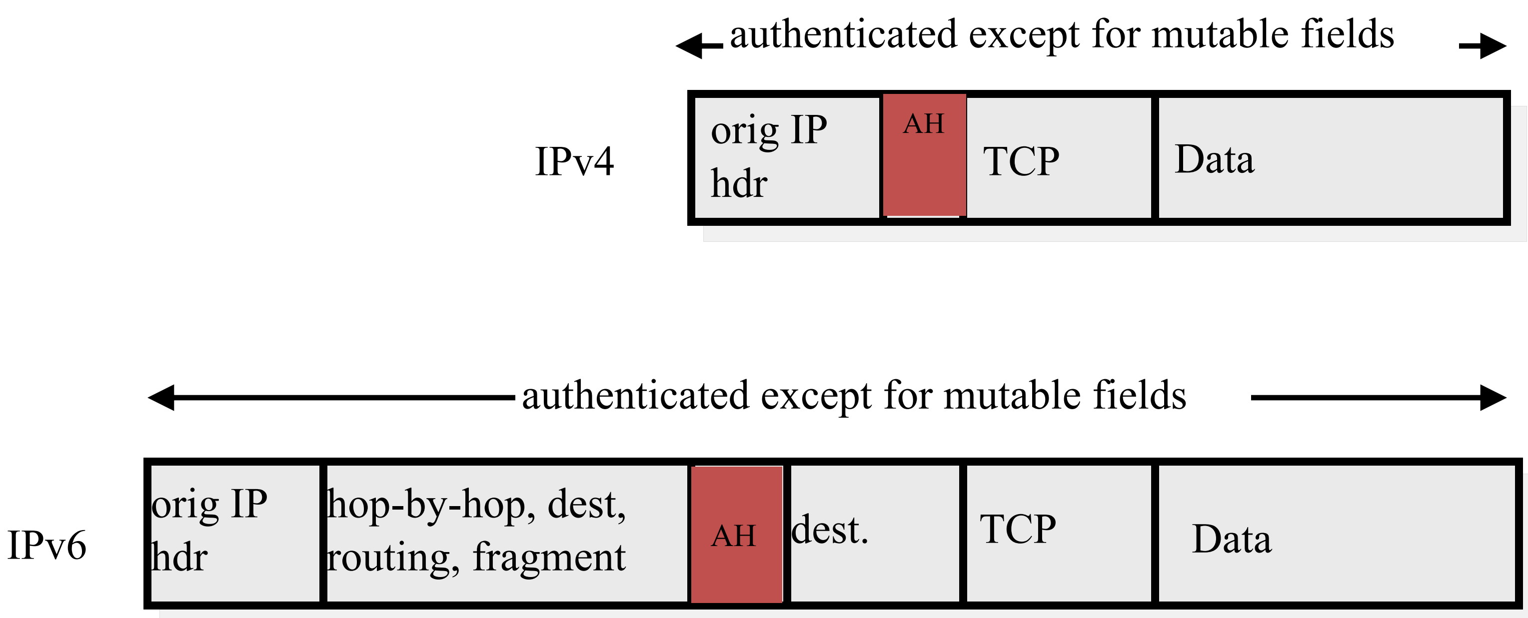
AH Protocol

- AH specifies a header added to IP datagrams.
- Fields in header include:
  - Payload length
  - SPI = Security Parameters Index
    - Identifies which algorithms and keys are to be used for IPSec processing (more later).
  - Sequence number
  - Authentication data (the MAC value)
    - Calculate over immutable IP header fields (so omit TTL) and payload or inner IP datagram.

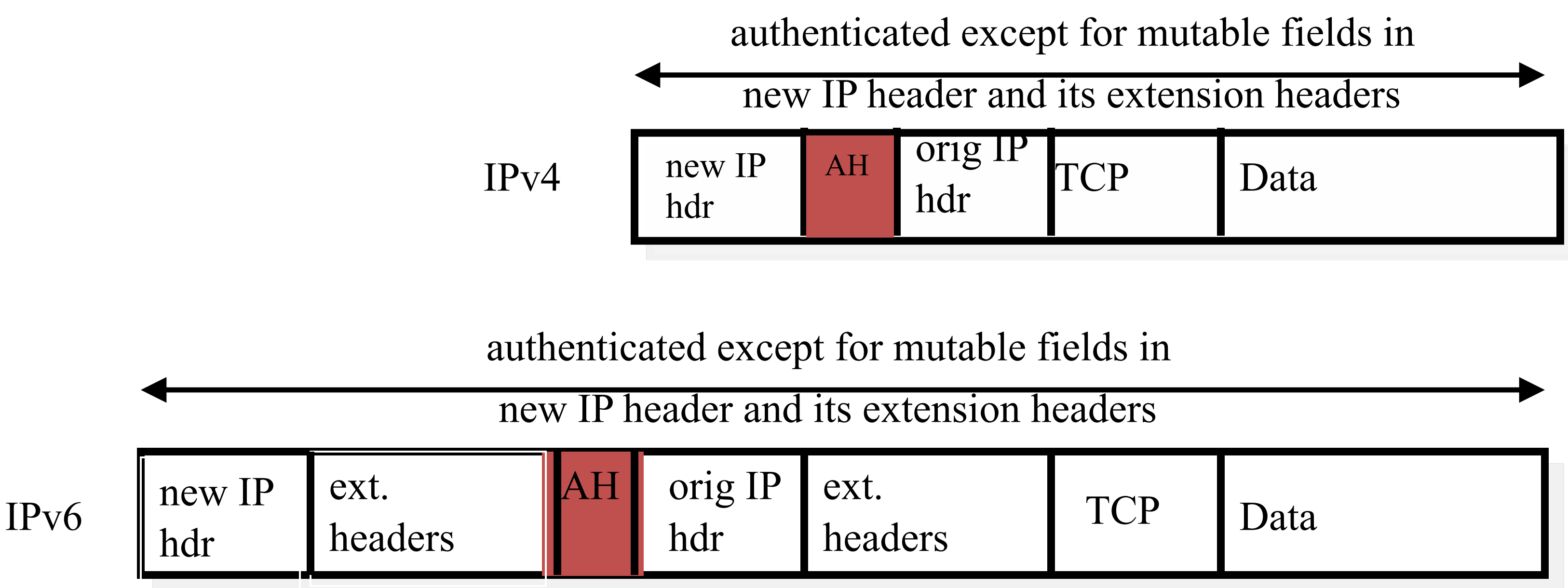
Before applying AH



Transport Mode (AH Authentication)



Tunnel Mode (AH Authentication)



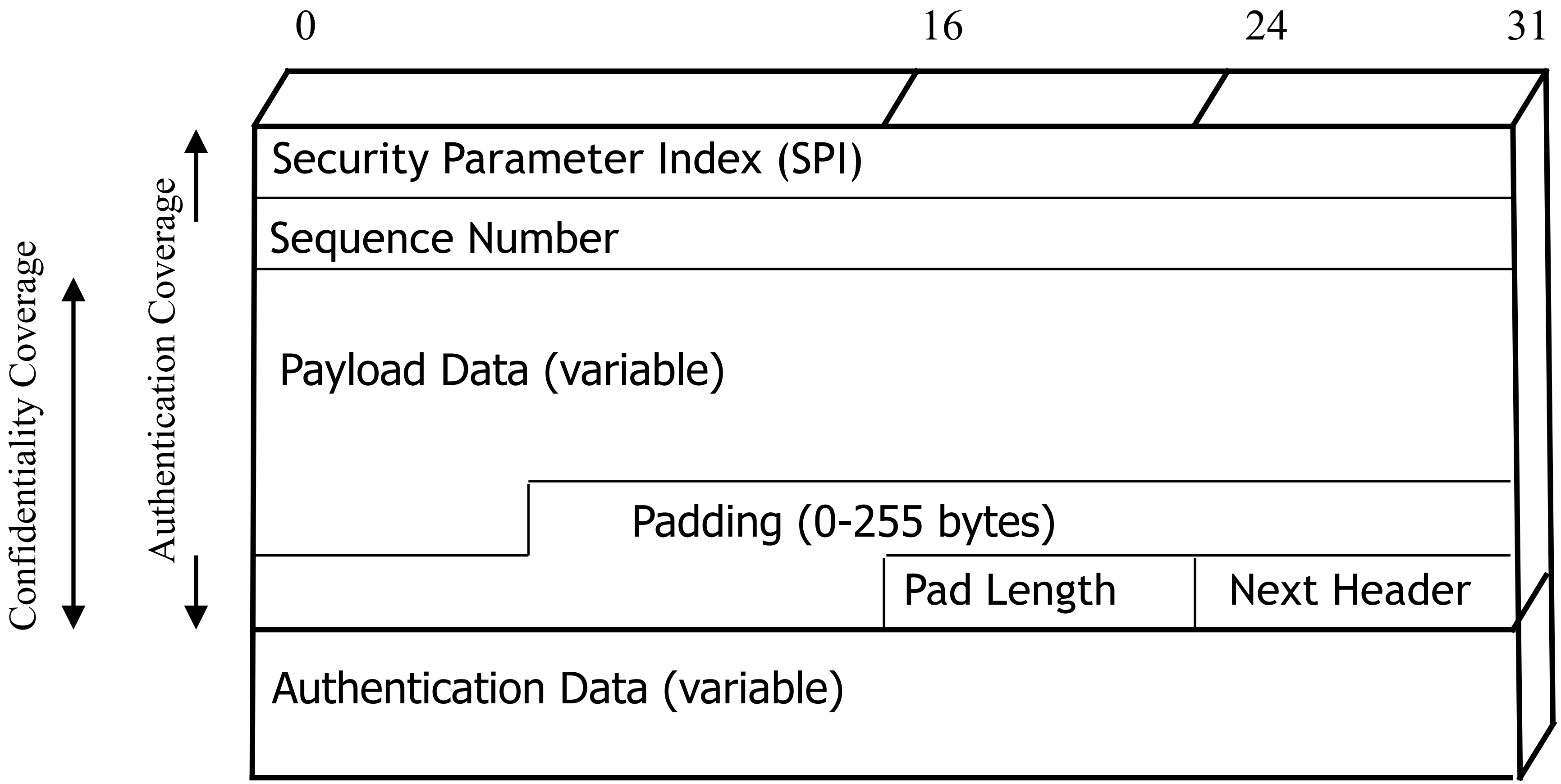
ESP Protocol

- ESP = Encapsulating Security Payload (RFC 2406).
- Provides one or both:
  - Confidentiality for payload/inner datagram; sequence number not protected by encryption.
  - Authentication of payload/inner datagram; but **not** of any header fields (original header or outer header).
- Traffic-flow confidentiality in tunnel mode.
- Uses symmetric encryption and MACs based on secret keys shared between endpoints.

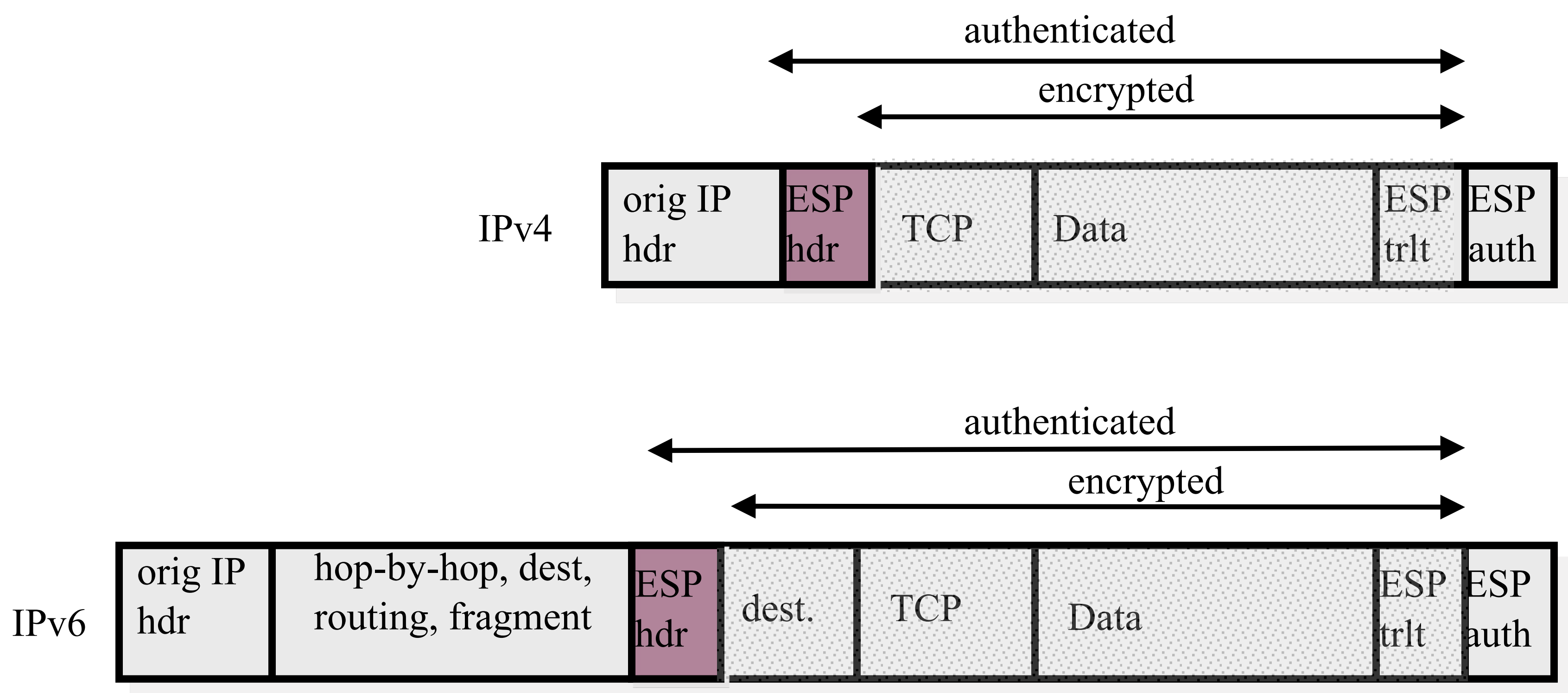
ESP Protocol

- ESP specifies a header and trailing fields to be added to IP datagrams.
- Header fields include:
  - SPI (Security Parameters Index): identifies which algorithms and keys are to be used for IPsec processing (more later).
  - Sequence number.
- Trailer fields include:
  - Any padding needed for encryption algorithm (may also help disguise payload length).
  - Padding length.
  - Authentication data (if any) – the MAC value.

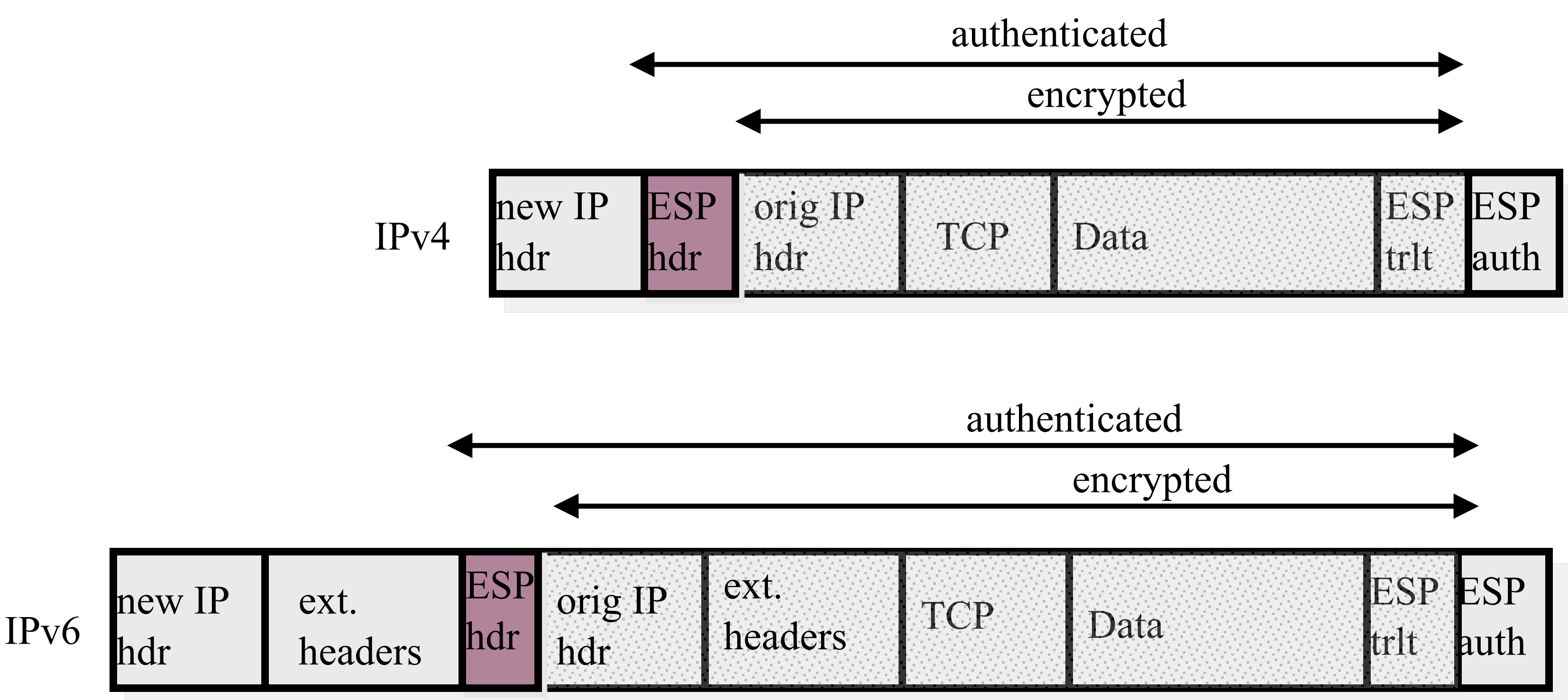
Encapsulating Security Payload



ESP Encryption and Authentication (Transport)



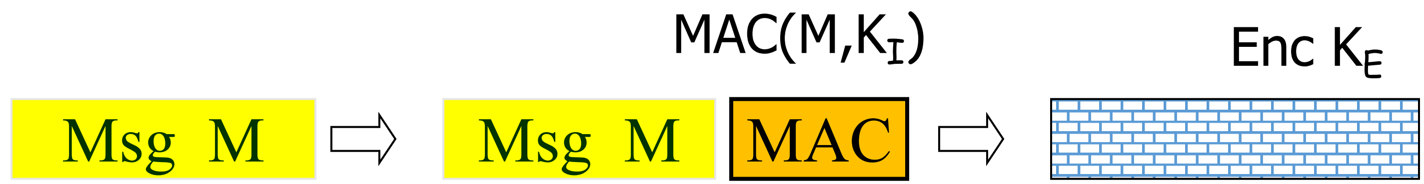
ESP Encryption and Authentication (Tunnel)



Combining MAC and ENC

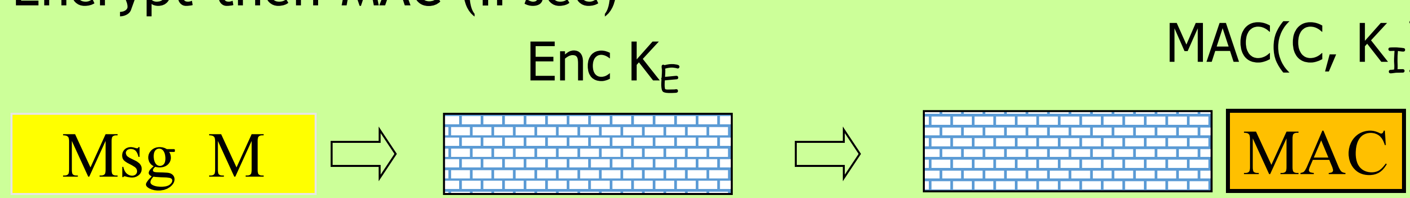
Encryption key K_E MAC key = K_I

Option 1: MAC-then-Encrypt (SSL)

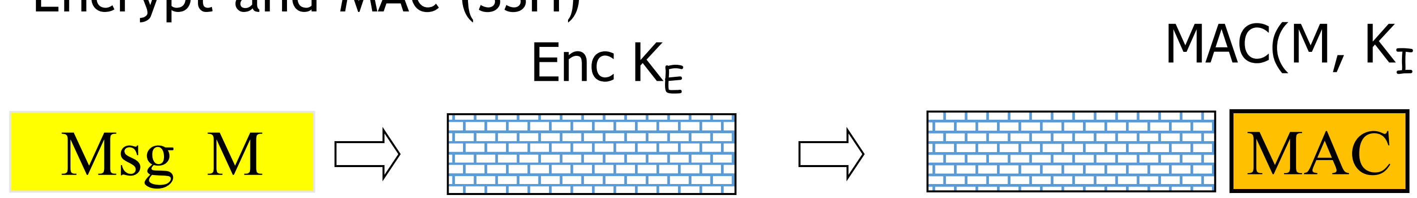


Option 2: Encrypt-then-MAC (IPsec)

Secure on general grounds



Option 3: Encrypt-and-MAC (SSH)

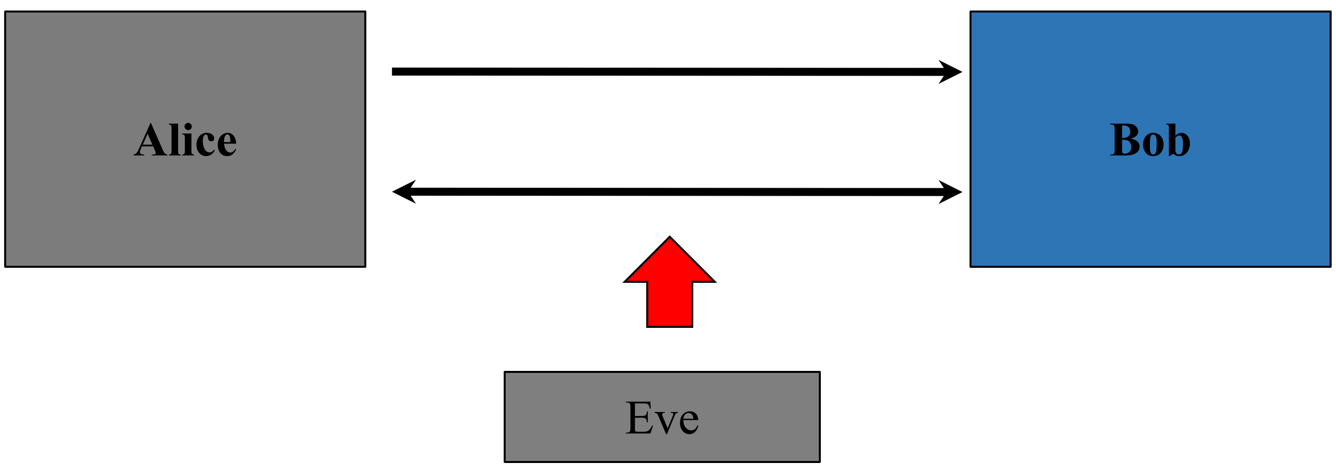


IPSec Key Management

- IPSec is a heavy consumer of symmetric keys:
  - One key for each SA.
  - Potentially, different SAs for every combination from:
    {ESP,AH} x {tunnel,transport} x {sender, receiver} x {protocol} x {port}.
- Where do these SAs and keys come from?
- Two sources:
  - Manual keying.
    - Fine for small number of nodes and testing purposes.
    - Hopeless for reasonably sized networks of IPSec-aware hosts.
  - IKE: Internet Key Exchange, RFC 2409.
    - RFC documentation hard to follow.
    - Algorithms and parameters negotiation
    - Protocols have many options and parameters.
  - IKEv2
    - Addresses problems and complexities of IKE (i.e. DoS).

Diffie-Hellman Protocol

- Simple public-key algorithm for key exchange
- Based on Discrete Logarithm Problem
- Secure against eavesdropping only



Authenticated DH: STS

- Use signature and proof of knowledge

$$A \xrightarrow{A,\ g^x} B$$

$$A \xleftarrow{B,\ g^y,\ \{SIG_B(g^x, g^y)\}_K} B$$

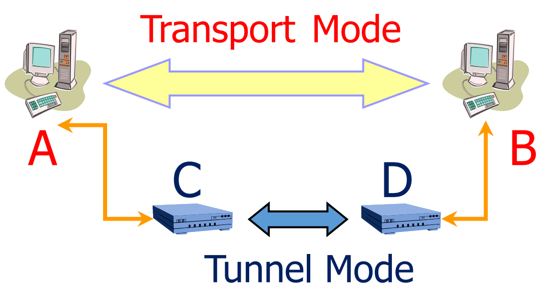
$$A \xrightarrow{\{SIG_A(g^y, g^x)\}_K} B$$

Note: power modulo p
p large prime and g is primitive root module p

SPD and SADB Example

SADB: Security Associations DB

SPD: Security Policies DB



A's SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

A's SADB

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

C's SPD

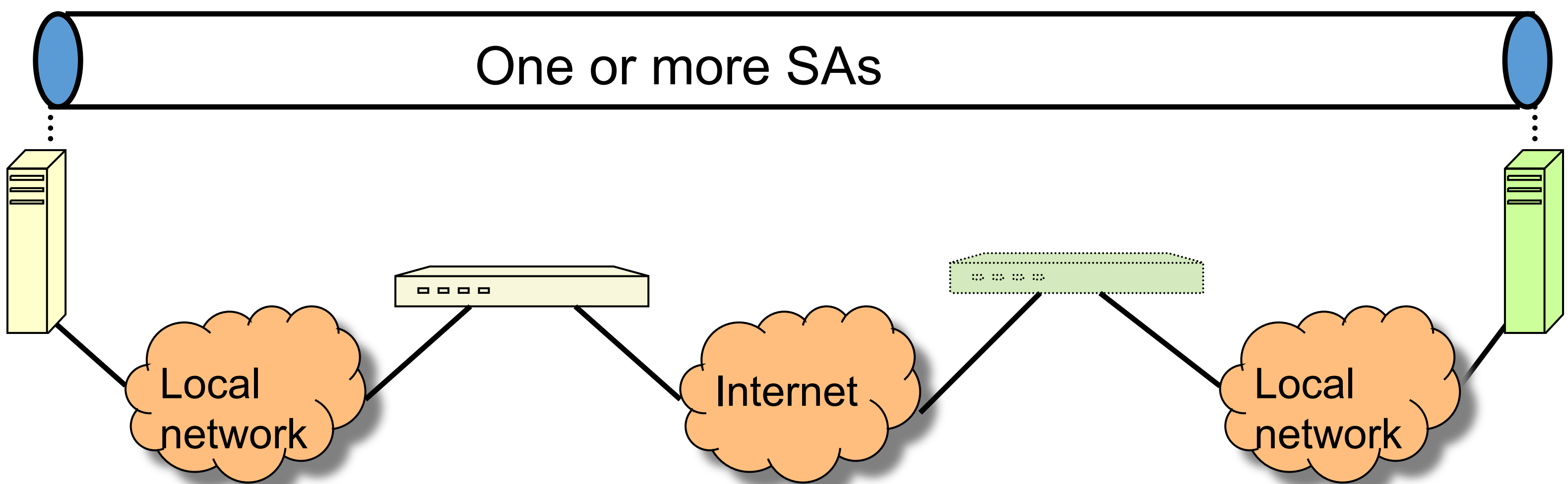
From	To	Protocol	Port	Policy	Tunnel Dest
		Any	Any	ESP[3DES]	D

C's SADB

From	To	Protocol	SPI	SA Record
		ESP	14	3DES key

Required SA Combinations

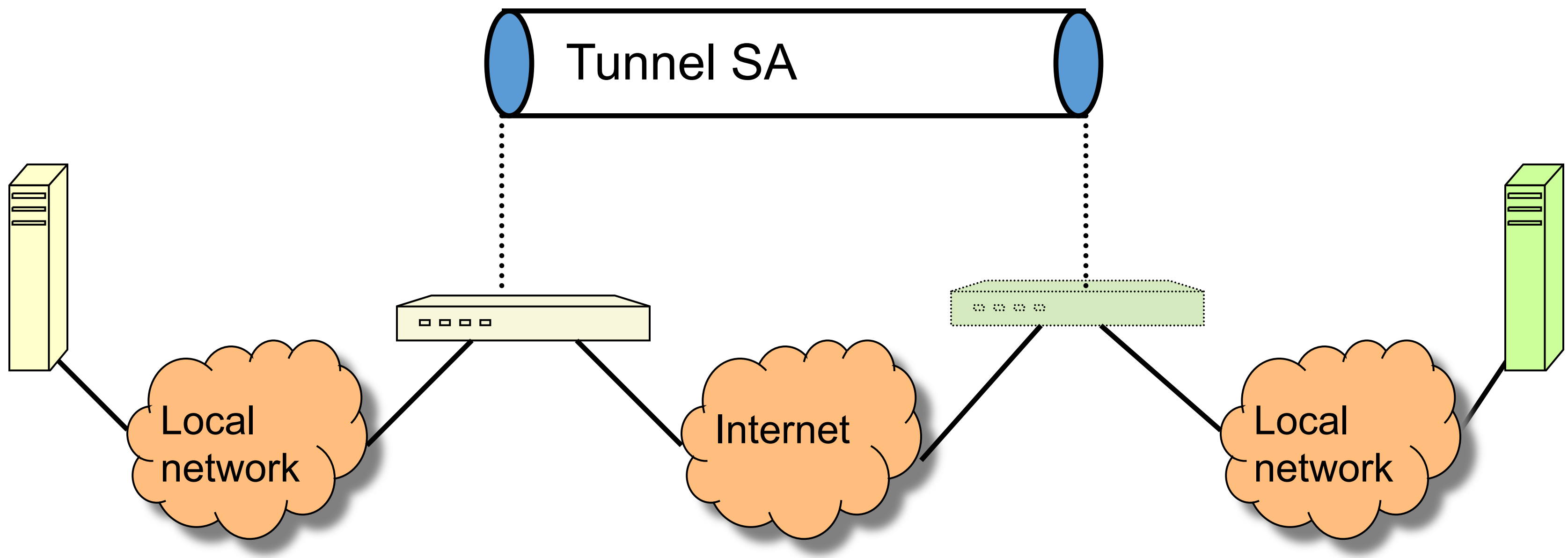
1. End-to-end application of IPsec between IPsec-aware hosts; one or more SAs, one of the following combinations:
   - AH in transport
   - ESP in transport
   - AH followed by ESP, both transport
   - Any of the above, tunnelled inside AH or ESP.



Required SA Combinations

2. Gateway-to-gateway only:

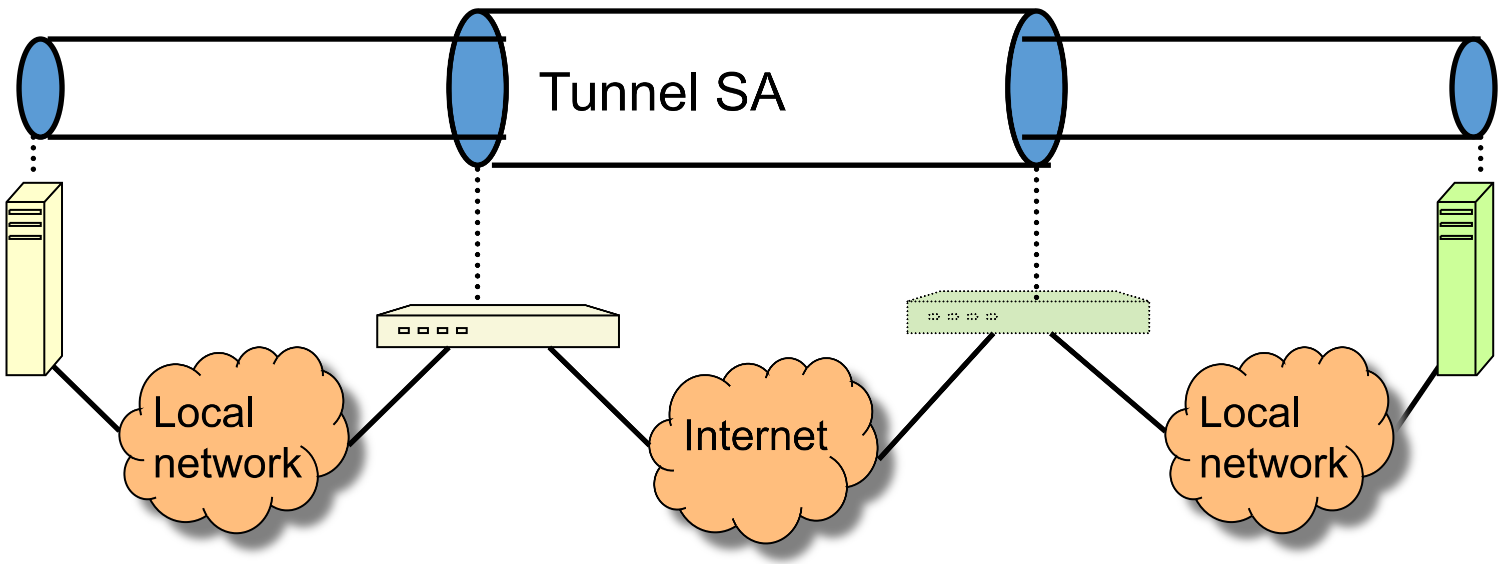
- No IPsec at hosts.
- Simple Virtual Private Network (VPN).
- Single tunnel SA supporting any of AH, ESP (conf only) or ESP (conf+auth).



UNIVERSITÀ DEGLI STUDI DI TRENTO

Required SA Combinations

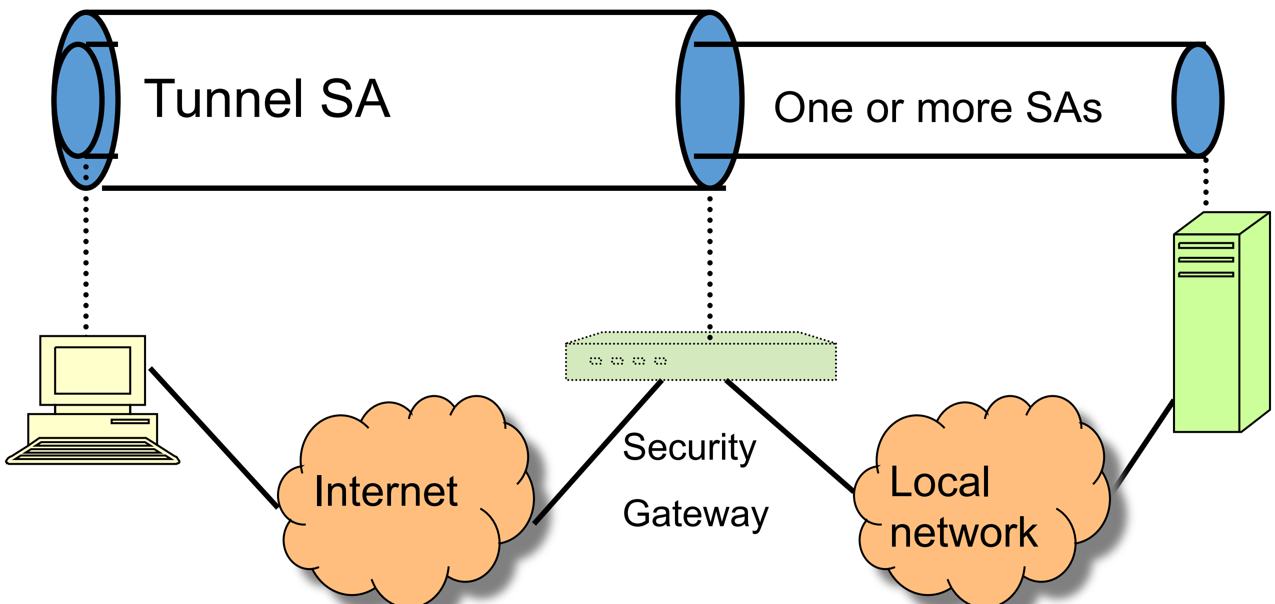
3. A combination of 1 and 2 above:
   - Gateway-to-gateway tunnel as in 2 carrying host-to-host traffic as in 1.
   - Gives additional, flexible security on local networks (between gateways and hosts)
   - E.g., ESP in tunnel mode carrying AH in transport mode.



Required SA Combinations

4. Remote host support:

- Single gateway (typically firewall).
- Remote host uses Internet to reach firewall, then gain access to server behind firewall.
- Traffic protected in inner tunnel to server as in case 1 above.
- Outer tunnel protects inner traffic over Internet.



Final Notes on IPSec

- IPSec and firewalls have problems working together.
  - Authentication of source IP addresses in AH is the issue.
  - Some firewalls change these addresses on out-bound datagrams (NAT).
- IPSec support for ICMP is somewhat complicated.
- Managing IPSec policy and deployments is tricky.
  - Getting it wrong can mean losing connectivity, e.g. by making exchanges of routing updates unreadable.
  - Getting it wrong can mean loss of security.
  - Many, many IPSec options, rather poor documentation.

IPSec documents:

- RFC 2401: An overview of security architecture
- RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
- RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
- RFC 2408: Specification of key managament capabilities

- and many more...

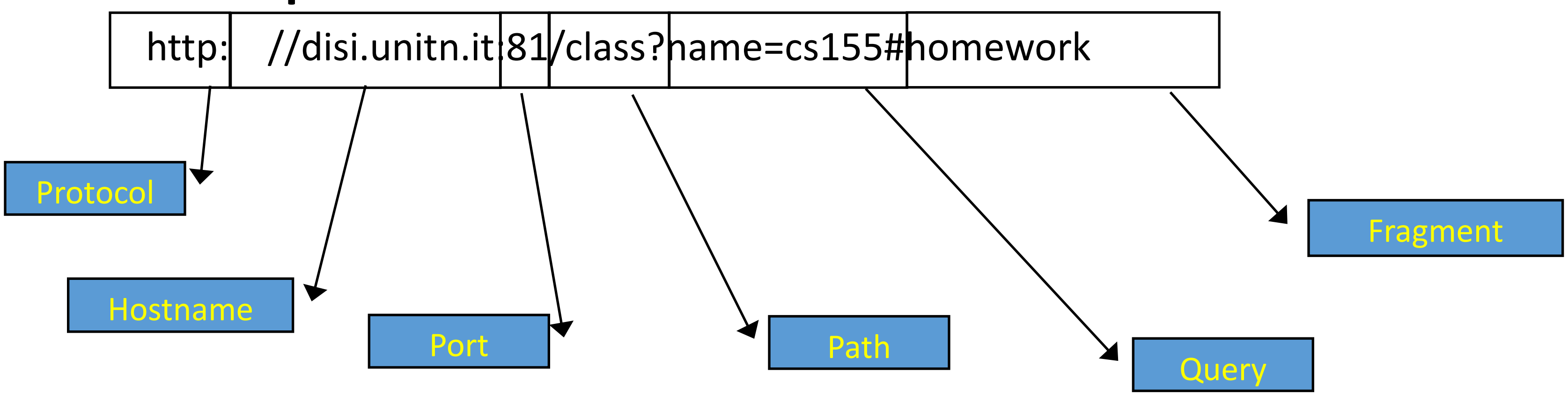
HTTP

- Main protocol on which the www works
- Based on the notion that client can either request or submit data to a server
- Two methods
  - GET → Requests data from a specified resource
    - GET /test/demo_form.asp**?name1=value1&name2=value2** HTTP/1.1
  - POST → Submits data to be processed to a specified resource
    - POST /test/demo_form.asp HTTP/1.1
      Host: w3schools.com
      name1=value1&name2=value2
- HTTP is stateless
  - HTTP cookies enable statefulness

URLs

- Global identifiers of network-retrievable documents

- **Example:**



- Special characters are encoded as hex:
  - %0A = newline
  - %20 or + = space, %2B = + (special exception)

HTTP GET Request

Method File Parameters HTTP version Headers

```
GET /index.php&user=luca&password=1234 HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)
Host: www.example.com
Referer: http://www.google.com?q=example
```

HTTP POST Request

Method File HTTP version Headers

```
POST /index.php HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)
Host: www.example.com
Referer: http://www.google.com?q=example
user=luca&password=1234
```

Parameters

HTTP Response

HTTP version Status code Reason phrase

Headers

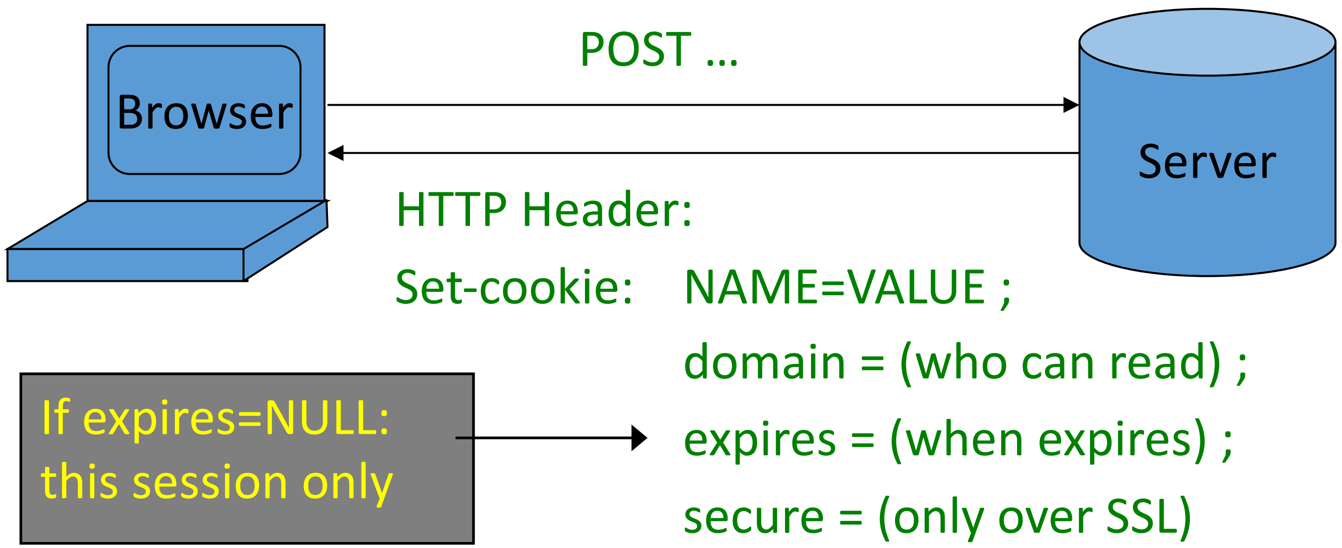
```
HTTP/1.1 200 OK
Date: Sun, 21 Apr 1996 02:20:42 GMT
Server: Microsoft-Internet-Information-Server/5.0
Connection: keep-alive
Content-Type: text/html
Last-Modified: Thu, 18 Apr 1996 17:39:05 GMT
Set-Cookie: …
Content-Length: 2543

<HTML> Some data... blah, blah, blah </HTML>
```

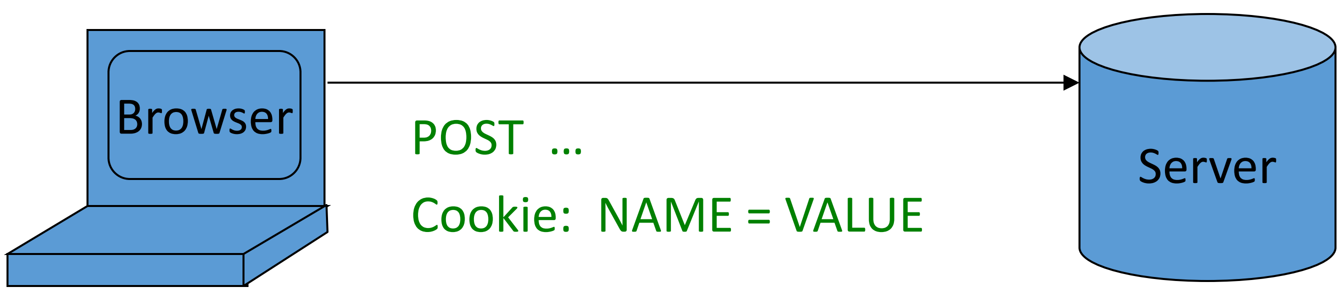
Data

Cookies

Cookies

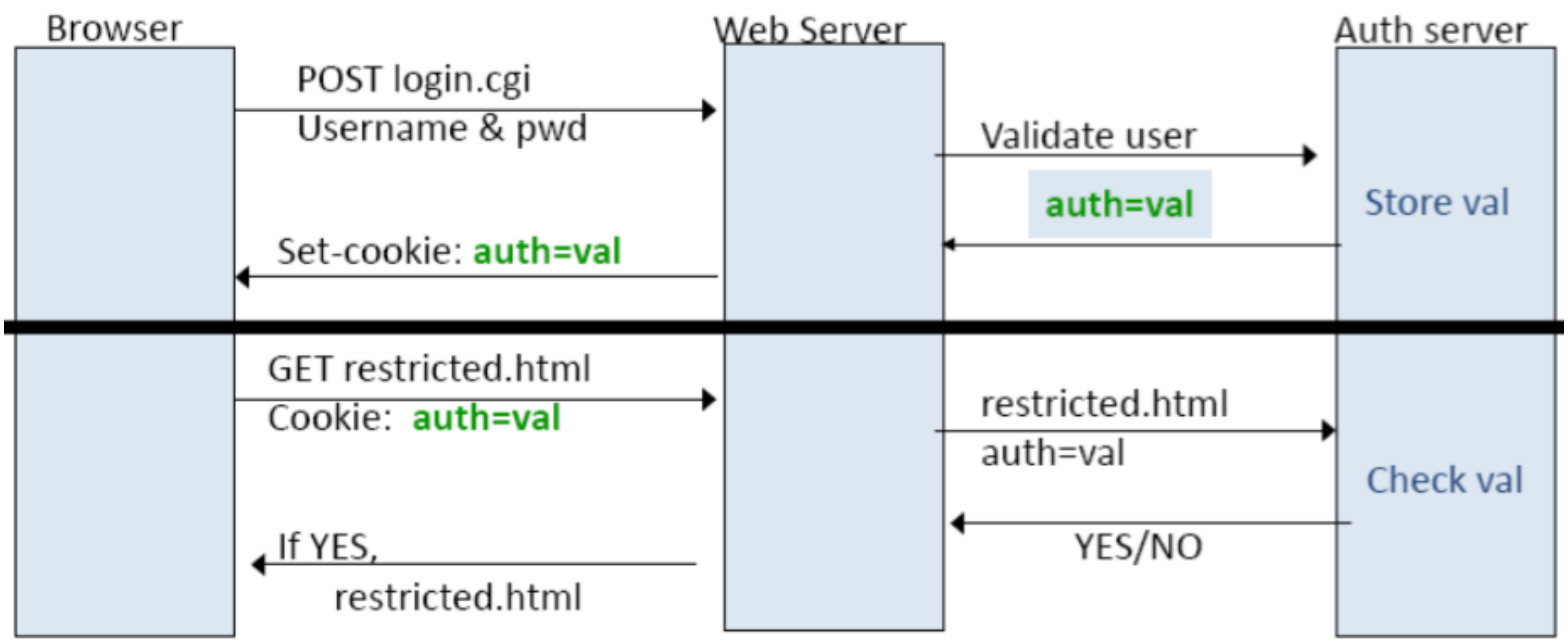
- Used to store state on user's machine



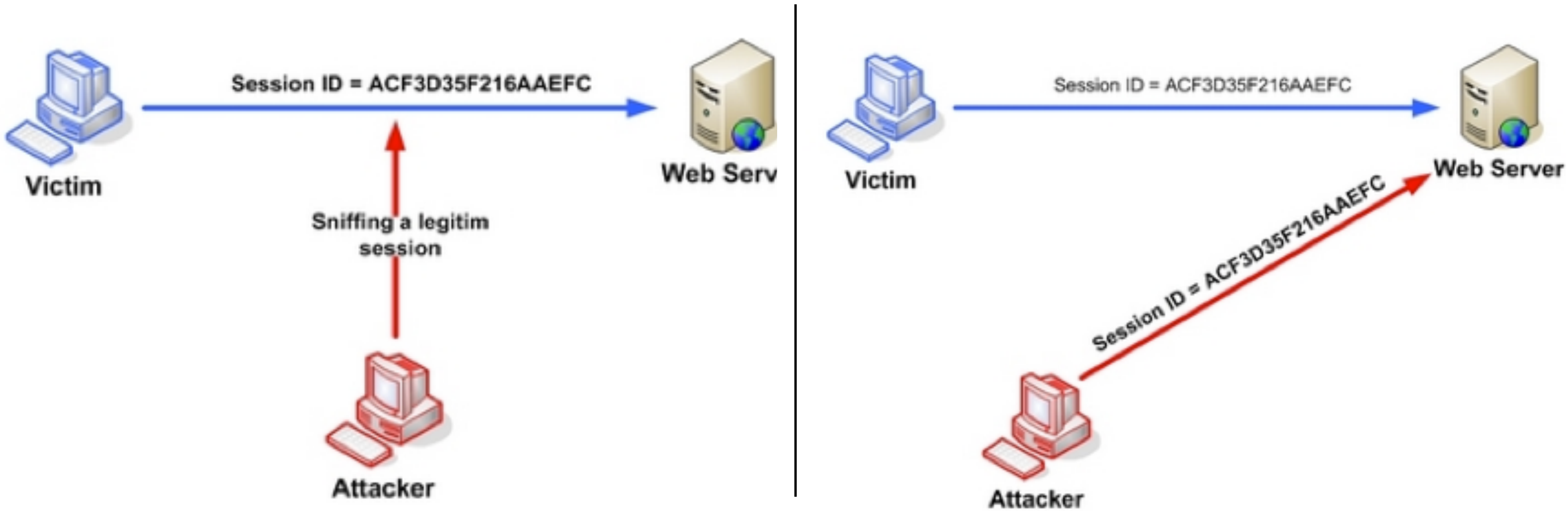


HTTP is stateless protocol; cookies add state

Cookie example: authentication

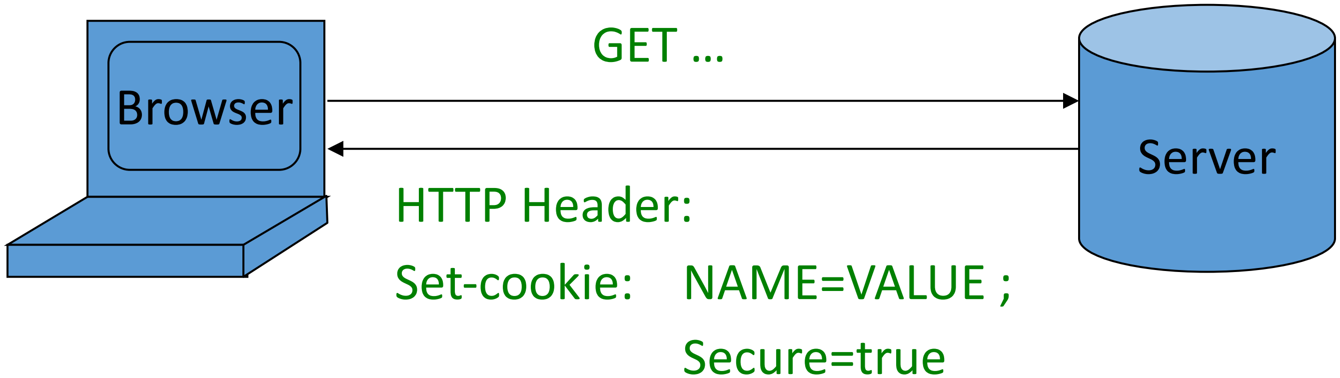


Attack example: HTTP session hijacking



- Session ID used by webserver to authenticate client "victim"
  - Send over cookie in-the-clear
- Attacker can read the session ID cookie and spoof the victim's identity
  - e.g. access to personal webpages/accounts (e.g. Facebook until 2011)
- https://www.owasp.org/index.php/Session_hijacking_attack

Secure Cookies



- Provides confidentiality against network attacker
  - Browser will only send cookie back over encrypted channels
- … but no integrity
  - Can rewrite secure cookies over HTTP

    ⇒⇒ network attacker can rewrite secure cookies

Suggested reading

- Bykova, Marina, and Shawn Ostermann. "Statistical analysis of malformed packets and their origins in the modern Internet." *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. ACM, 2002.
- Hao Yang ; Osterweil, E. ; Massey, D. ; Songwu Lu ; Lixia Zhang. Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing. Vol 8, Issue 5.*
- Internet Census 2012. Port scanning /0 using insecure embedded devices.
  - http://internetcensus2012.bitbucket.org/paper.html
- Blackert, W. J., et al. "Analyzing interaction between distributed denial of service attacks and mitigation technologies." *DARPA information survivability conference and exposition, 2003. Proceedings*. Vol. 1. IEEE, 2003.
- S. M. Bellovin. 1989. Security problems in the TCP/IP protocol suite. *SIGCOMM Comput. Commun. Rev.* 19, 2 (April 1989), 32-48. DOI=http://dx.doi.org/10.1145/378444.378449