IP Security

- Chapter 6 of William Stallings. Network Security Essentials (2nd edition). Prentice Hall. 2003.

Slides by Henric Johnson

Blekinge Institute of Technology, Sweden

http://www.its.bth.se/staff/hjo/

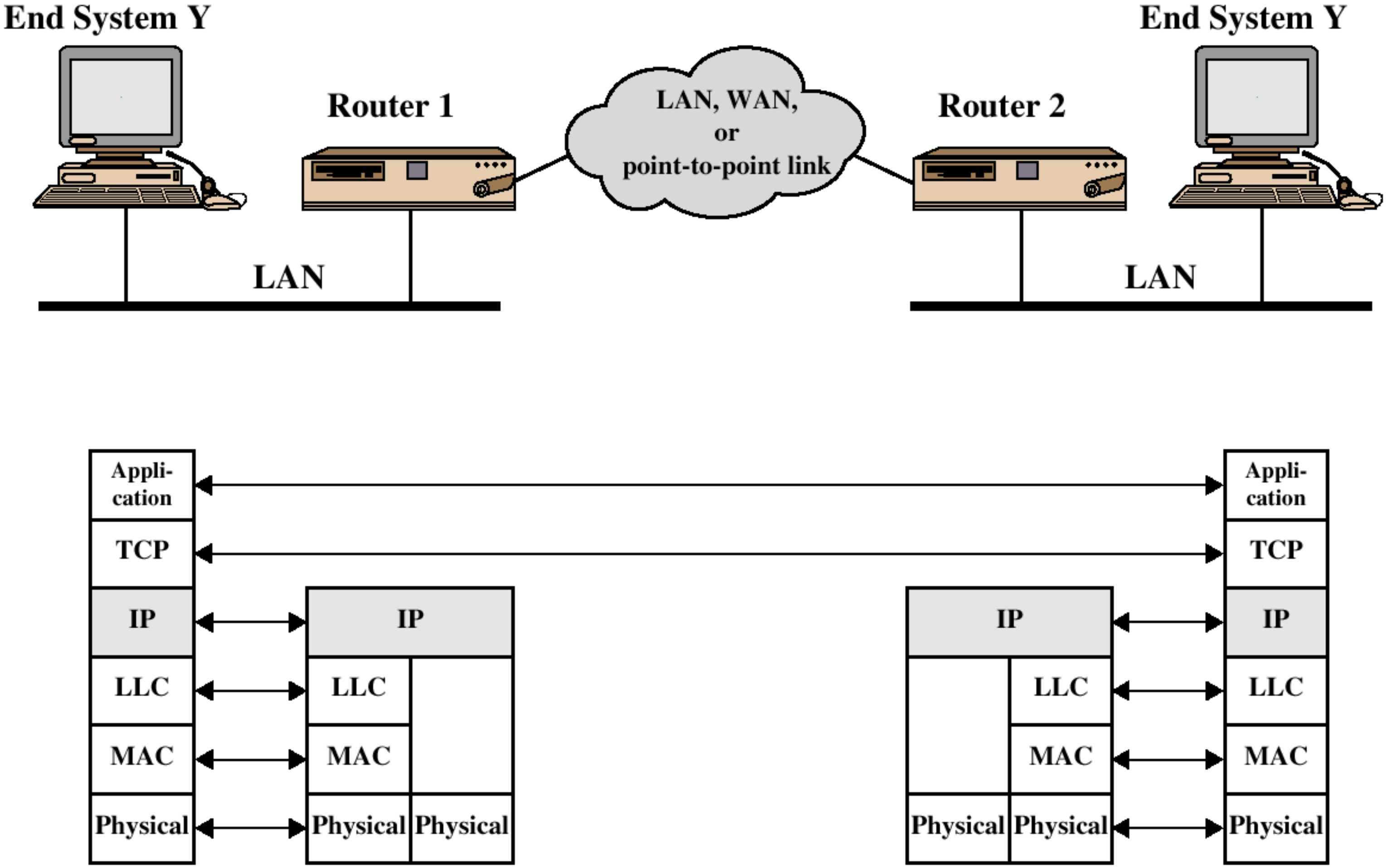
henric.johnson@bth.se

Revised by Andrew Yang

Outline

- Internetworking and Internet Protocols
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combinations of Security Associations
- Key Management

TCP/IP Example



End System Y

Router 1

LAN, WAN, or point-to-point link

Router 2

End System Y

LAN

LAN

Application

TCP

IP

LLC

MAC

Physical

IP

LLC

MAC

Physical

Physical

IP

LLC

MAC

Physical

Physical

Application

TCP

IP

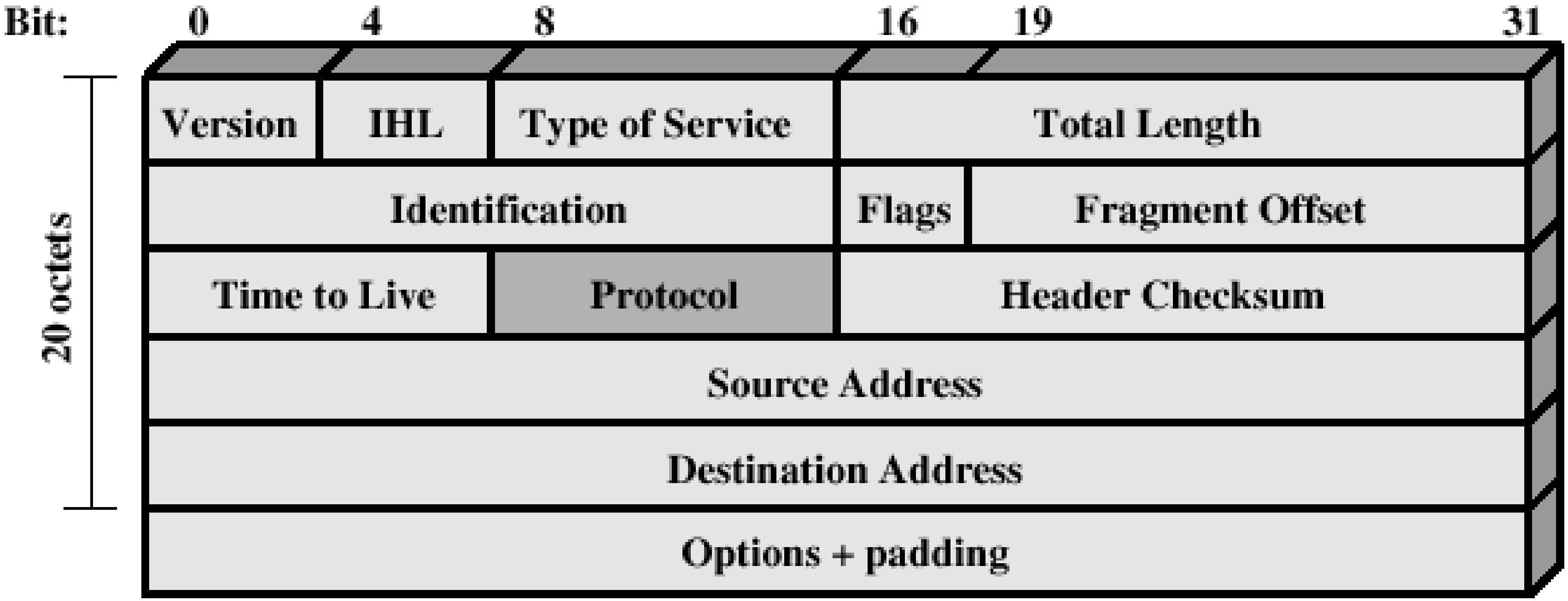
LLC

MAC

Physical

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

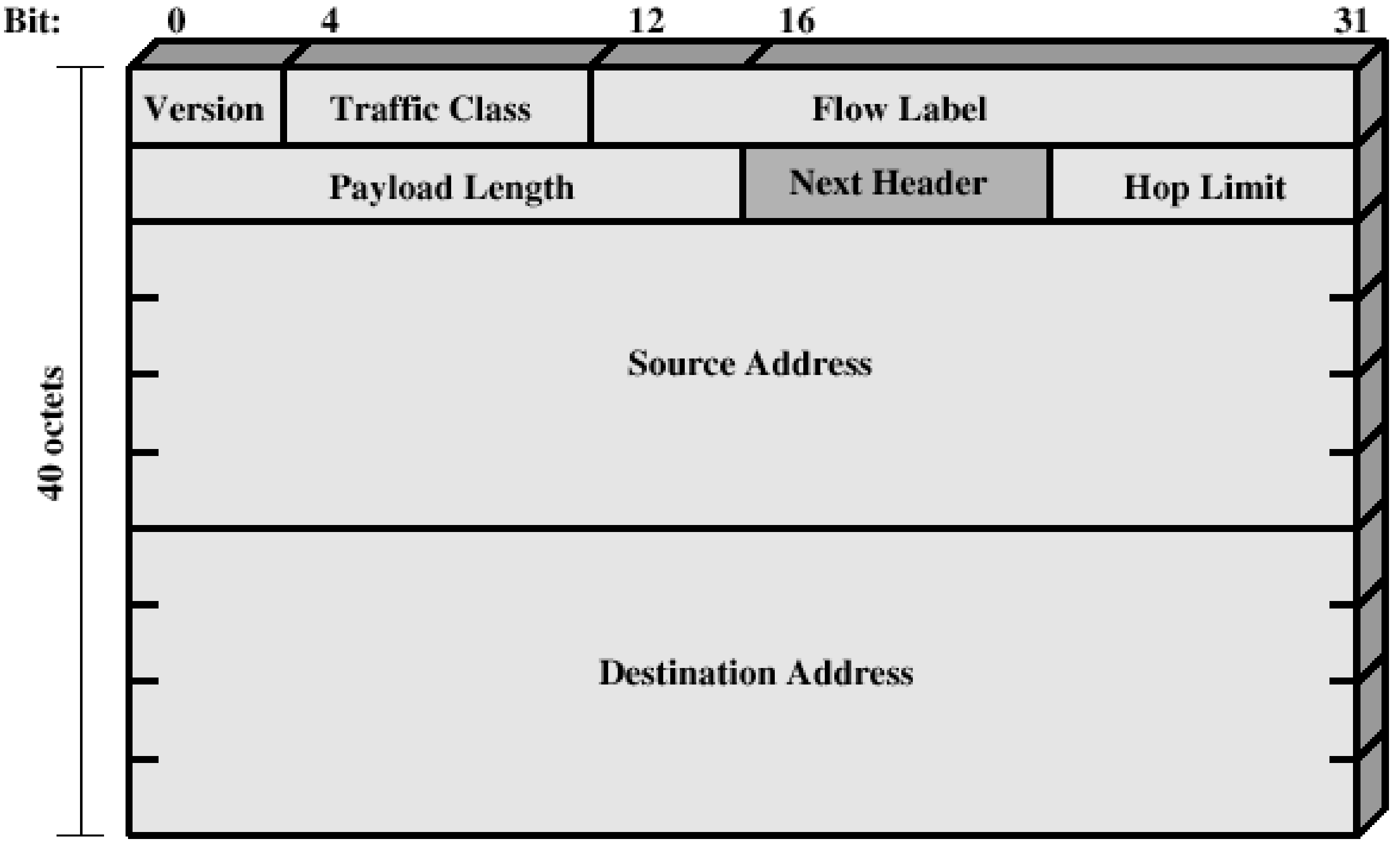
IPv4 Header



<table>
<tr><th>Bit:</th><th>0</th><th>4</th><th>8</th><th>16</th><th>19 … 31</th></tr>
<tr><td rowspan="5">20 octets</td><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td></td><td colspan="5">Options + padding</td></tr>
</table>

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

IPv6 Header



Bit: 0 4 12 16 31

Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source Address

Destination Address

40 octets

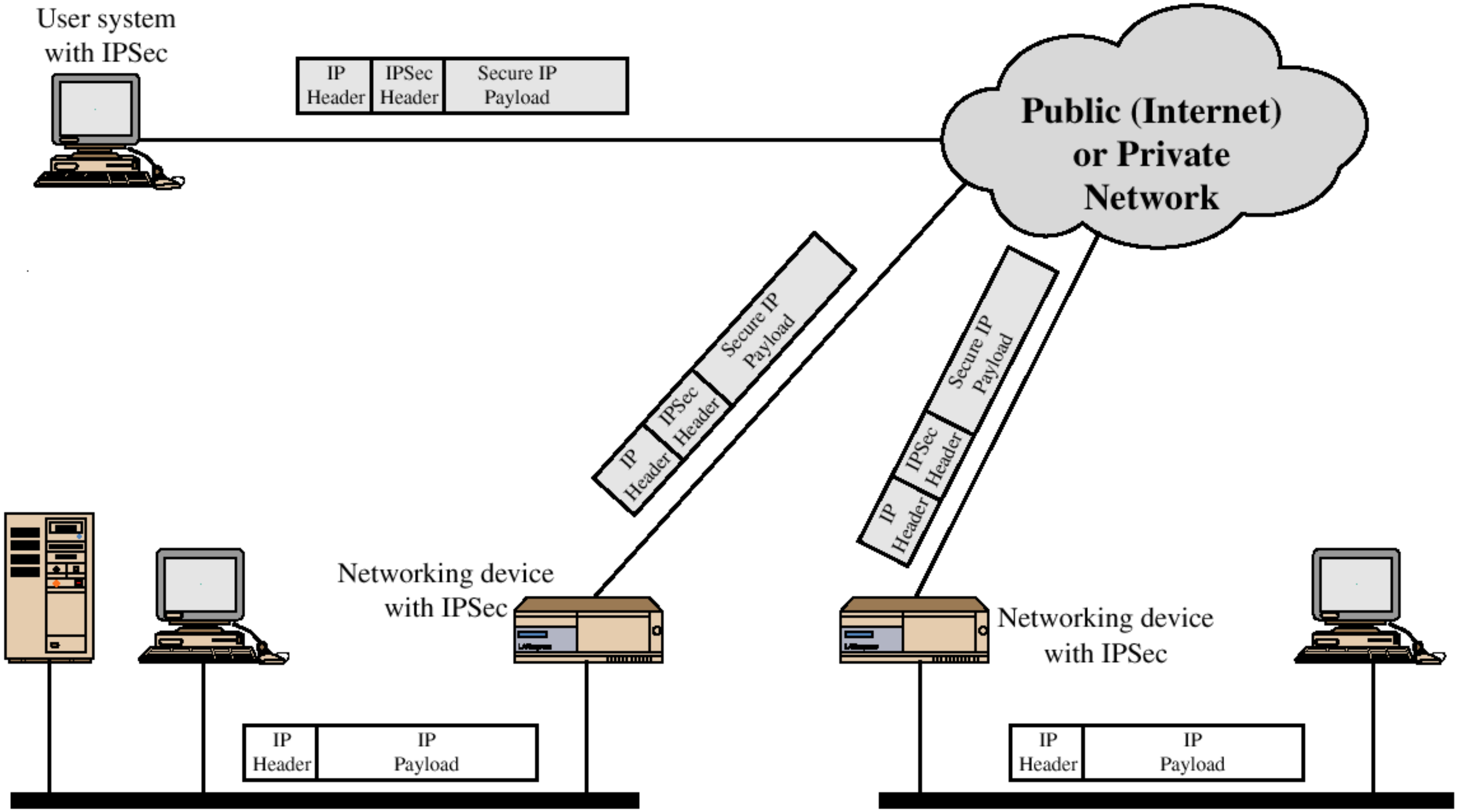
http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

IP Security Overview

- IPSec is not a single protocol.
- Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms to provide security appropriate for the communication.

- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establsihing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security

IP Security Scenario



http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

IP Security Overview

- Benefits of IPSec
  - Transparent to applications - below transport layer (TCP, UDP)
  - Provide security for individual users
- IPSec can assure that:
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

IP Security Architecture

- IPSec documents: NEW updates in 2005!
  - RFC 2401: **Security Architecture for the Internet Protocol.** S. Kent, R. Atkinson. November 1998. (An overview of security architecture) → RFC 4301 (12/2005)
  - RFC 2402: **IP Authentication Header.** S. Kent, R. Atkinson. November 1998. (Description of a packet encryption extension to IPv4 and IPv6) → RFC 4302 (12/2005)
  - RFC 2406: **IP Encapsulating Security Payload (ESP).** S. Kent, R. Atkinson. November 1998. (Description of a packet emcryption extension to IPv4 and IPv6) → RFC 4303 (12/2005)
  - RFC2407 **The Internet IP Security Domain of Interpretation for ISAKMP** D. Piper. November 1998. PROPOSED STANDARD. (Obsoleted by RFC4306)
  - RFC 2408: **Internet Security Association and Key Management Protocol (ISAKMP).** D. Maughan, M. Schertler, M. Schneider, J. Turner. November 1998. (Specification of key managament capabilities) (Obsoleted by RFC4306)
  - RFC2409 **The Internet Key Exchange (IKE)** D. Harkins, D. Carrel. November 1998. PROPOSED STANDARD. (Obsoleted by RFC4306, Updated by RFC4109)

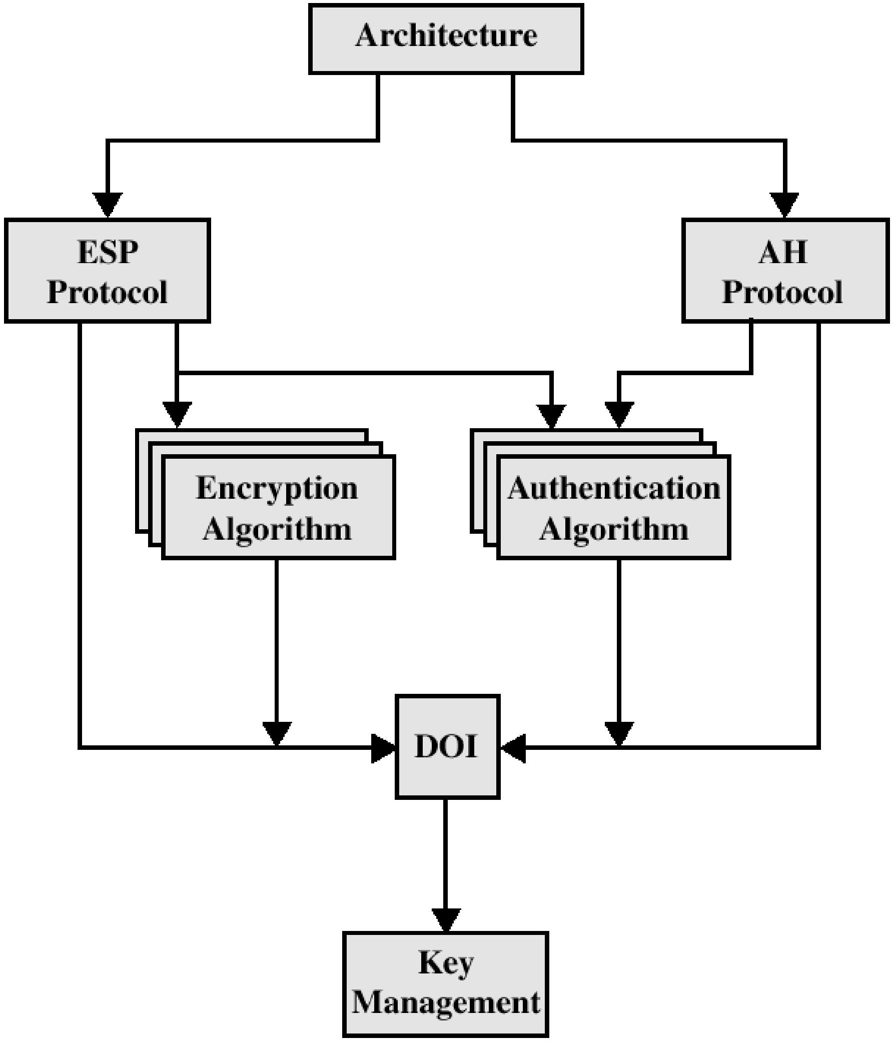
IP Security Architecture

- Internet Key Exchange (IKE)

  A method for establishing a security association (SA) that **authenticates users**, **negotiates the encryption method** and **exchanges the secret key**. IKE is used in the IPsec protocol. Derived from the ISAKMP framework for key exchange and the Oakley and SKEME key exchange techniques, IKE uses public key cryptography to provide the secure transmission of the secret key to the recipient so that the encrypted data may be decrypted at the other end. (http://computing-dictionary.thefreedictionary.com/IKE)

- RFC4306 **Internet Key Exchange (IKEv2) Protocol** C. Kaufman, Ed. December 2005 (Obsoletes RFC2407, RFC2408, RFC2409) PROPOSED STANDARD
- RFC4109 **Algorithms for Internet Key Exchange version 1 (IKEv1)** P. Hoffman. May 2005 (Updates RFC2409) PROPOSED STANDARD

IPSec Document Overview



http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

IPSec Services

- Access Control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiallity

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

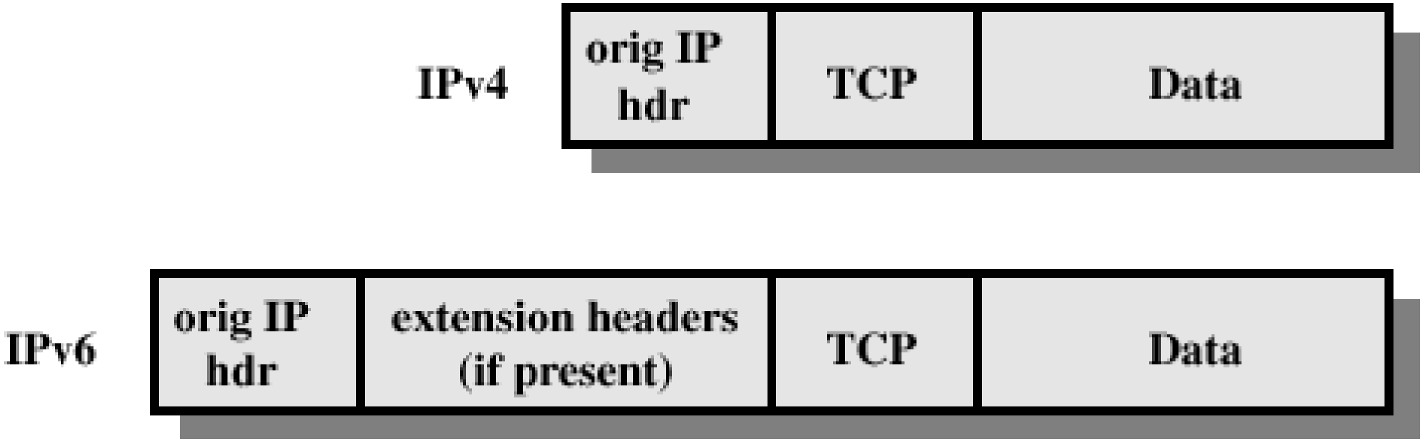
Security Associations (SA)

- A one way relationsship between a sender and a receiver.
- Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
  - Security Protocol Identifier

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

	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 plus selected portions of outer IP header
ESP	**Encrypts** IP payload and any IPv6 extesion header	**Encrypts** inner IP packet
ESP with authentication	**Encrypts** IP payload and any IPv6 extesion header. **Authenticates** IP payload but no IP header	**Encrypts** inner IP packet. **Authenticates** inner IP packet.

Before applying AH



IPv4

orig IP hdr

TCP

Data

IPv6

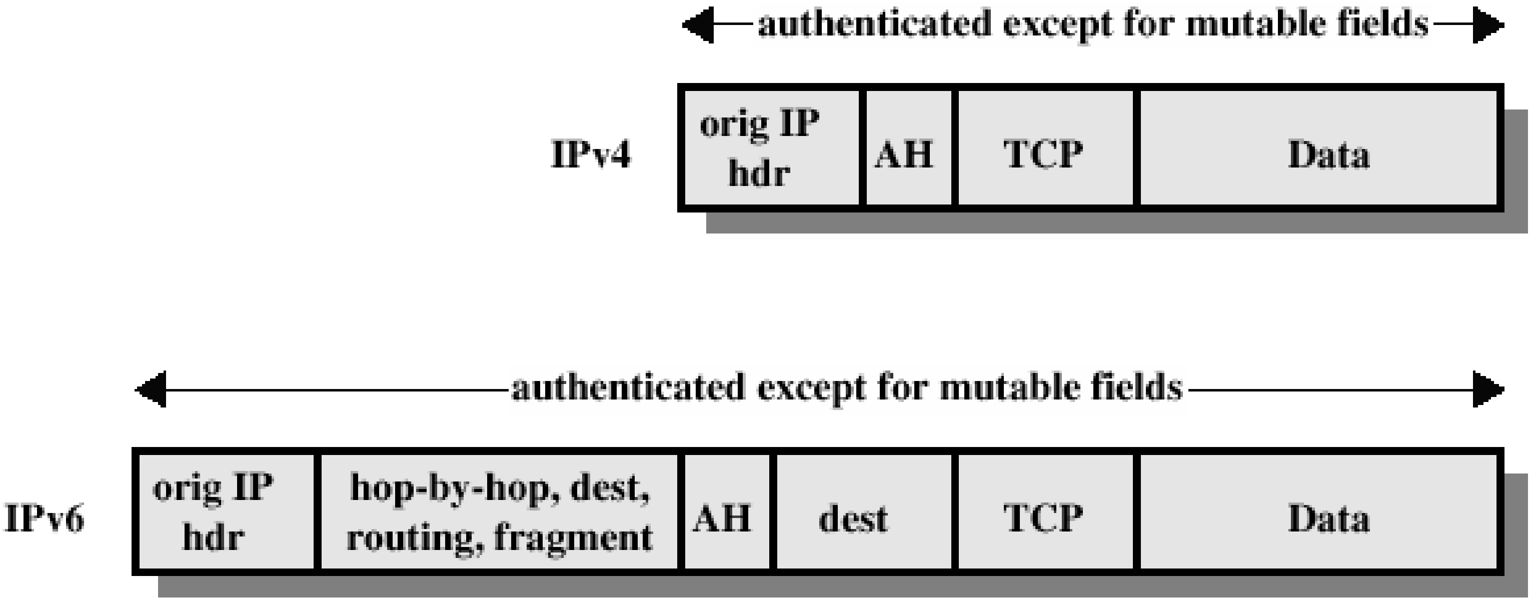
orig IP hdr

extension headers (if present)

TCP

Data

Transport Mode
(AH Authentication)



authenticated except for mutable fields

IPv4

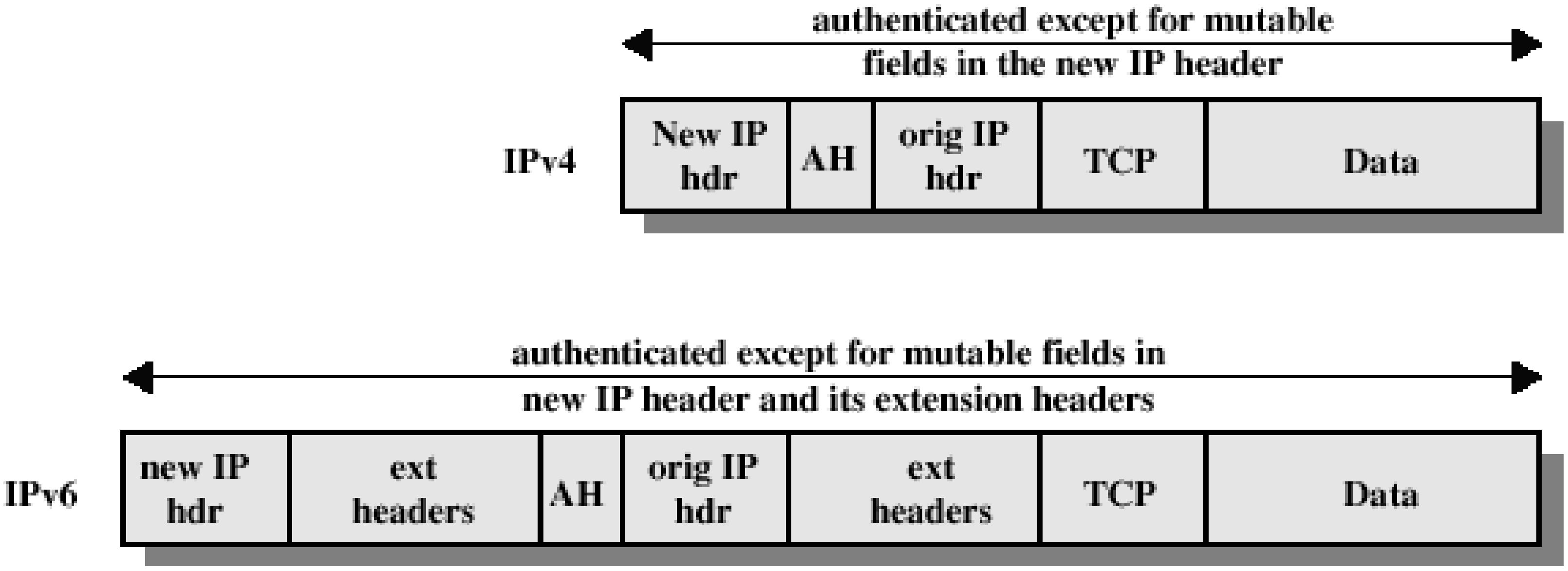
orig IP hdr | AH | TCP | Data

authenticated except for mutable fields

IPv6

orig IP hdr | hop-by-hop, dest, routing, fragment | AH | dest | TCP | Data

Tunnel Mode (AH Authentication)



authenticated except for mutable fields in the new IP header

IPv4

New IP hdr | AH | orig IP hdr | TCP | Data

authenticated except for mutable fields in new IP header and its extension headers

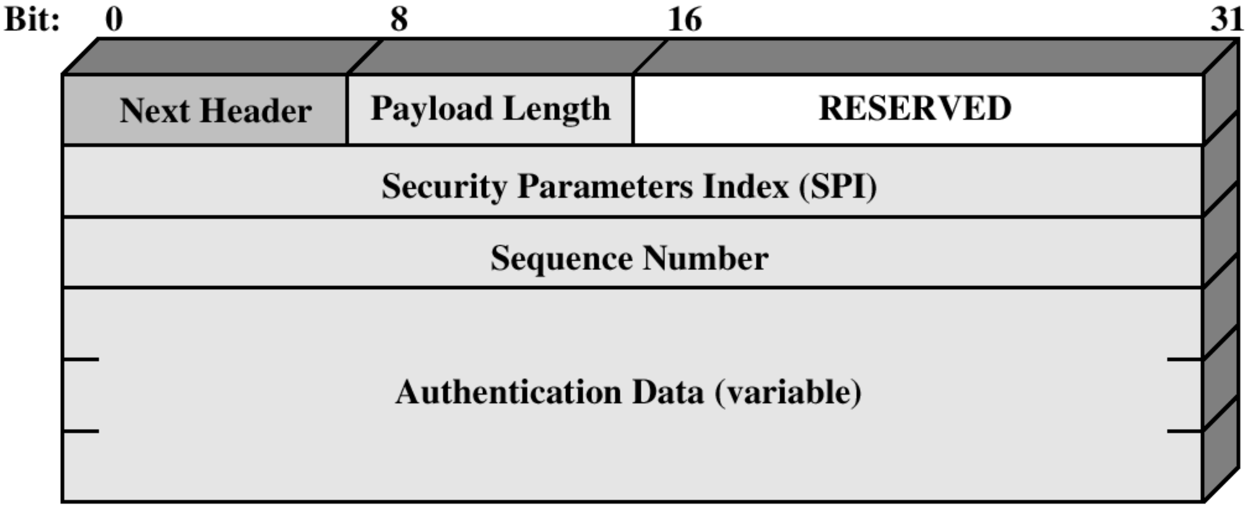
IPv6

new IP hdr | ext headers | AH | orig IP hdr | ext headers | TCP | Data

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

Authentication Header

- Provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks.



Next Header | Payload Length | RESERVED

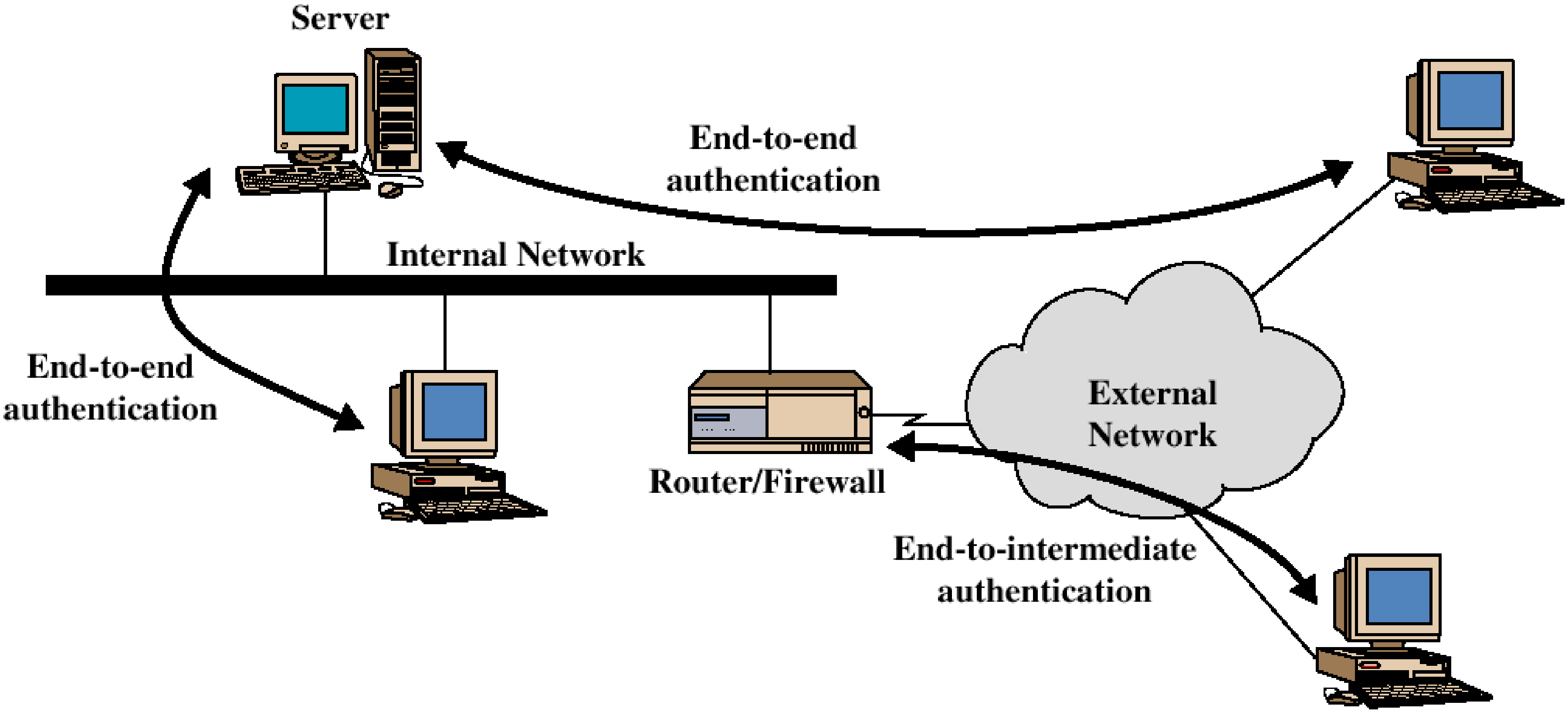
Security Parameters Index (SPI)

Sequence Number

Authentication Data (variable)

Figure 6.3 IPSec Authentication Header

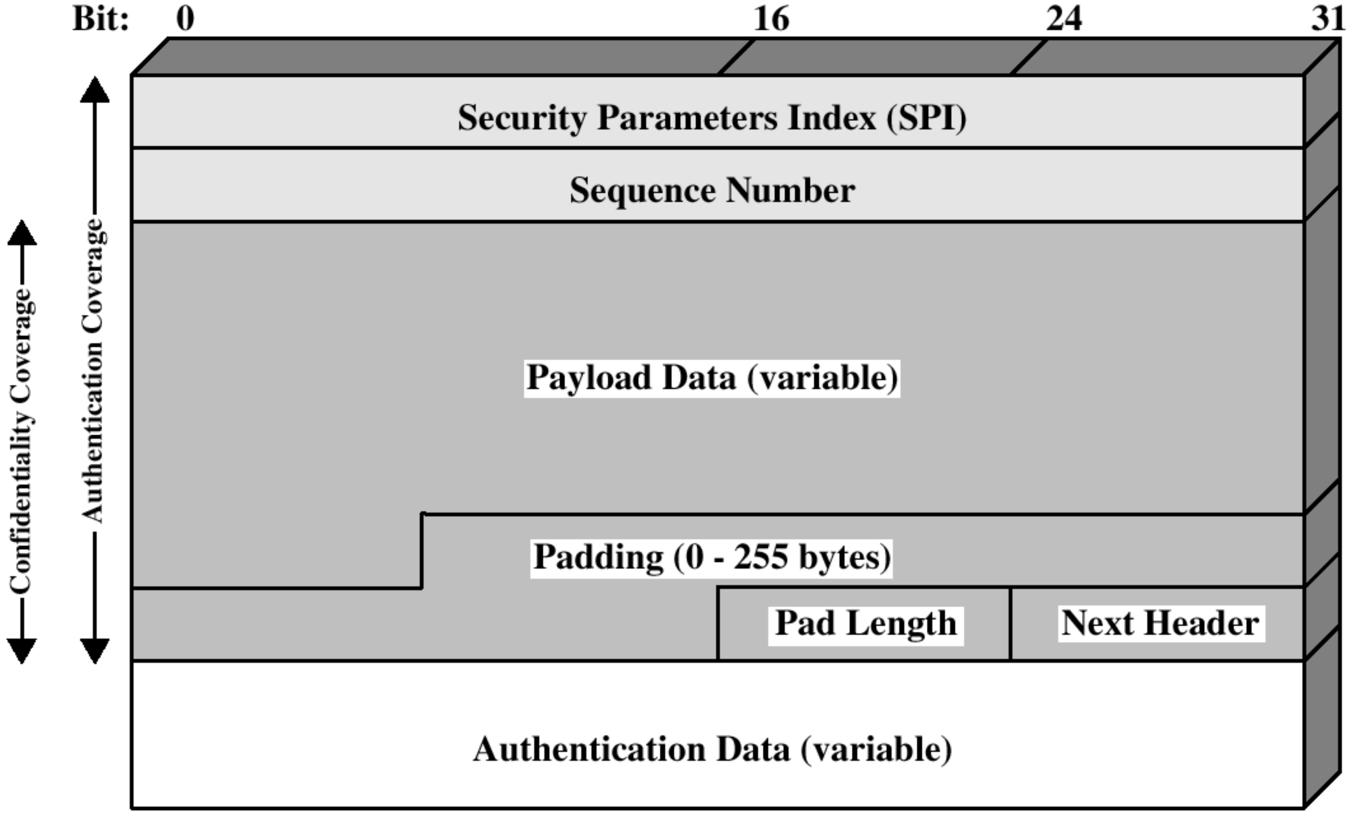
End-to-end versus End-to-Intermediate Authentication



http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

Encapsulating Security Payload

- ESP provides confidentiality services



Bit: 0 16 24 31

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding (0 - 255 bytes)

Pad Length

Next Header

Authentication Data (variable)

Confidentiality Coverage

Authentication Coverage

Figure 6.7 IPSec ESP Format

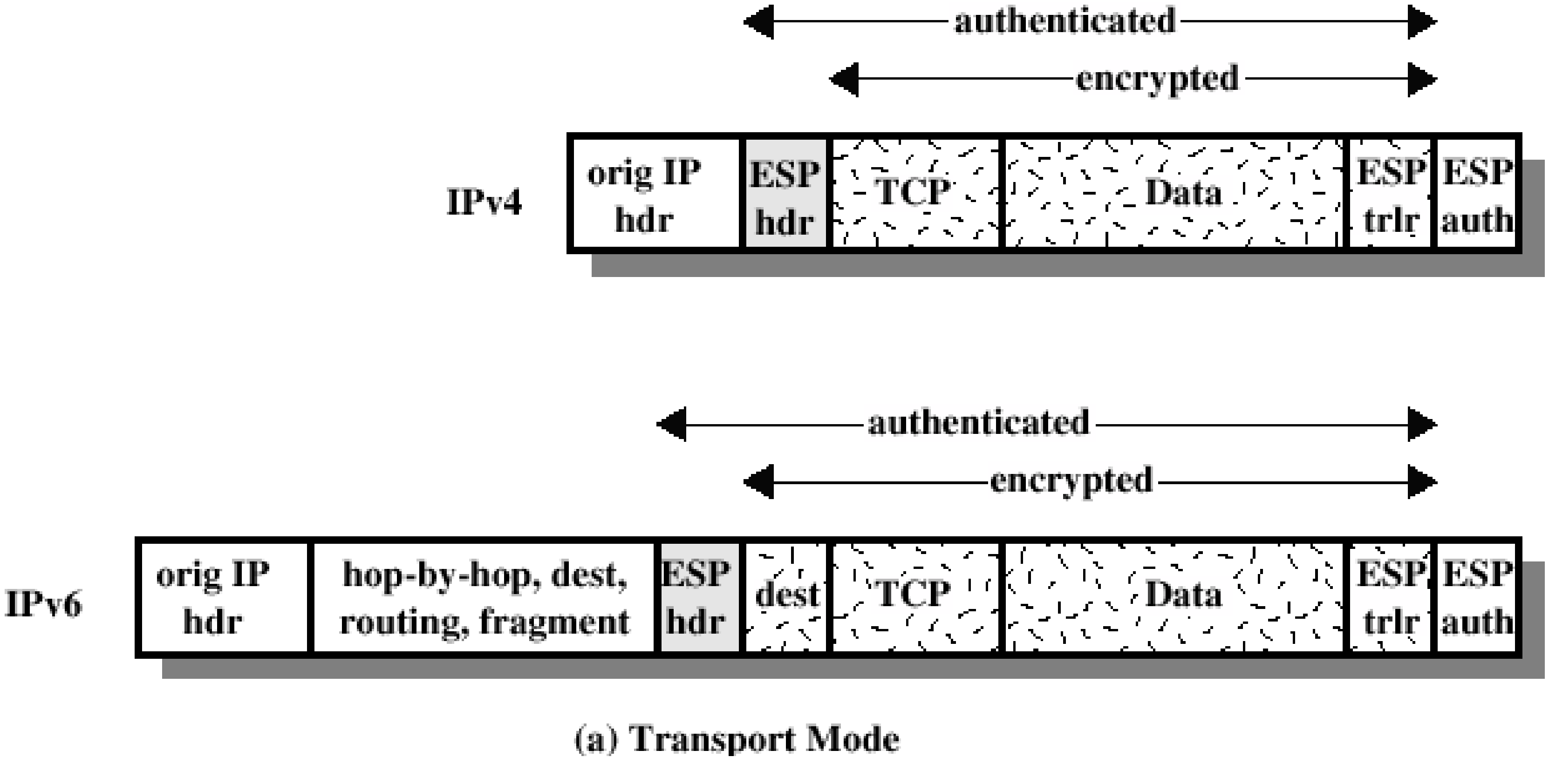
/IPsecurity.ppt

Encryption and Authentication Algorithms

- Encryption:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- Authentication:
  - HMAC-MD5-96
  - HMAC-SHA-1-96

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

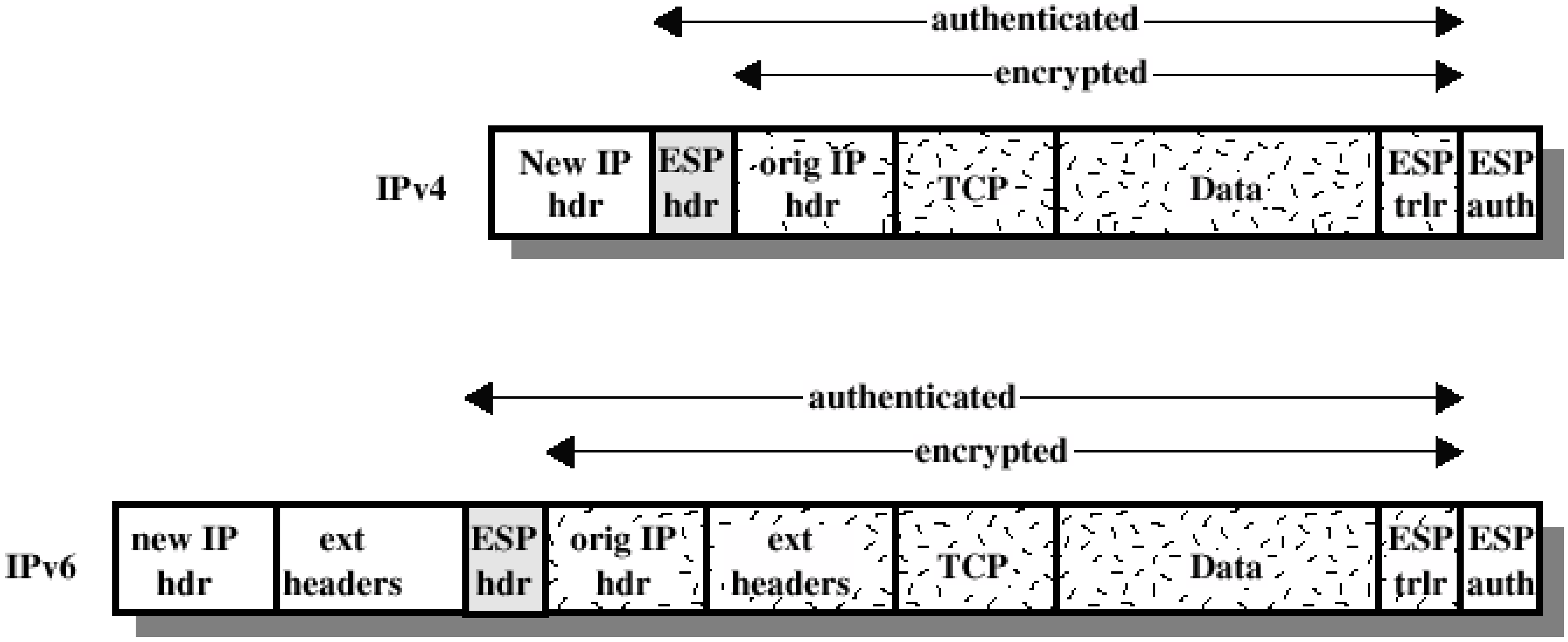
ESP Encryption and Authentication



(a) Transport Mode

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

ESP Encryption and Authentication



(b) Tunnel Mode

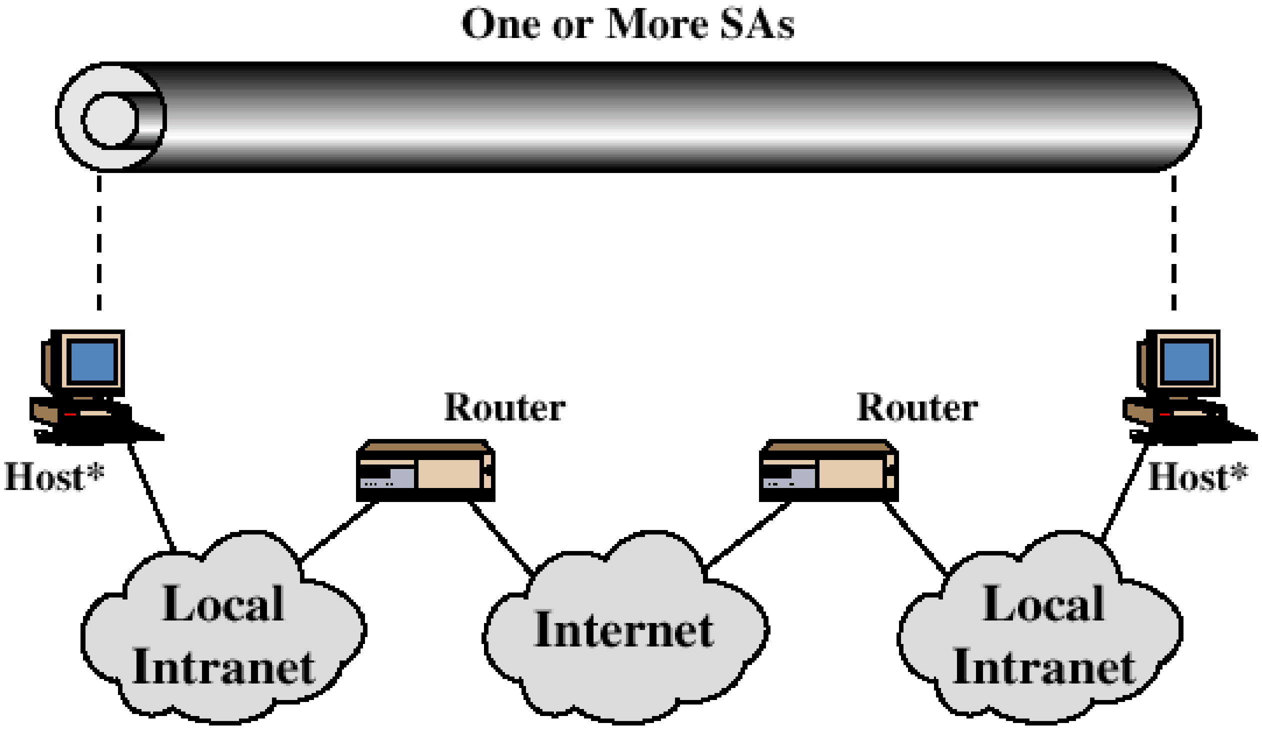
Security Associations (SA)

- a set of policy and key(s) used to protect information in an association
- Examples: ESP, AH, IKE

  "IKE performs mutual authentication between two parties and establishes an IKE **Security Association (SA)** that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload (ESP) [ESP] or Authentication Header (AH) [AH] and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry." – (RFC 7296)

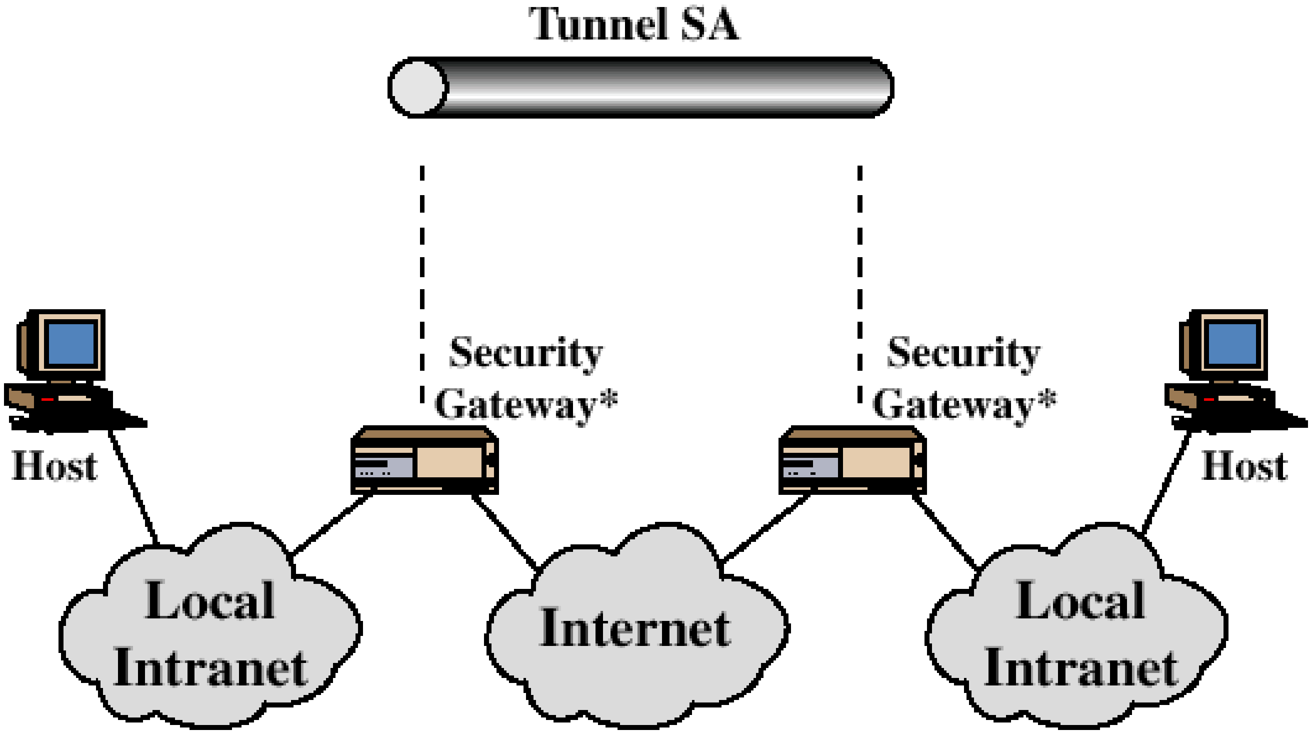
- Multiple SAs are often combined to achieve goals.
  – Next several slides

Combinations of Security Associations



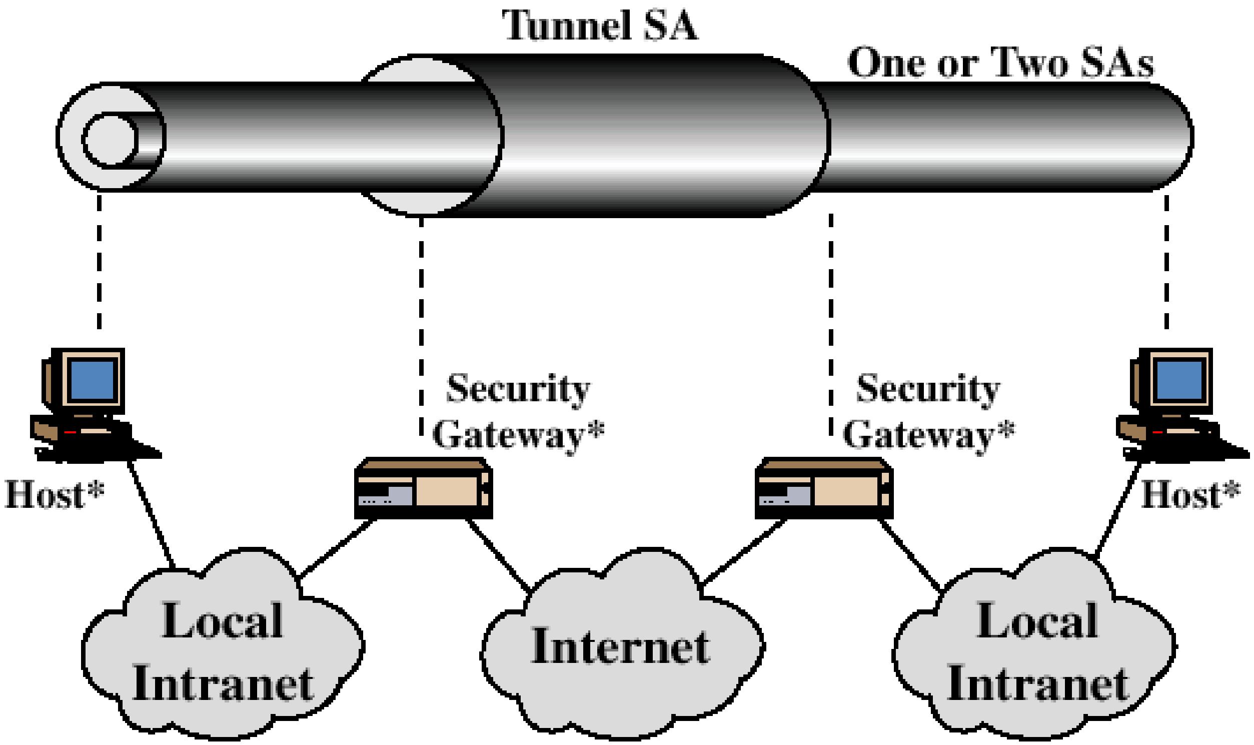
(a) Case 1

Combinations of Security Associations



(b) Case 2

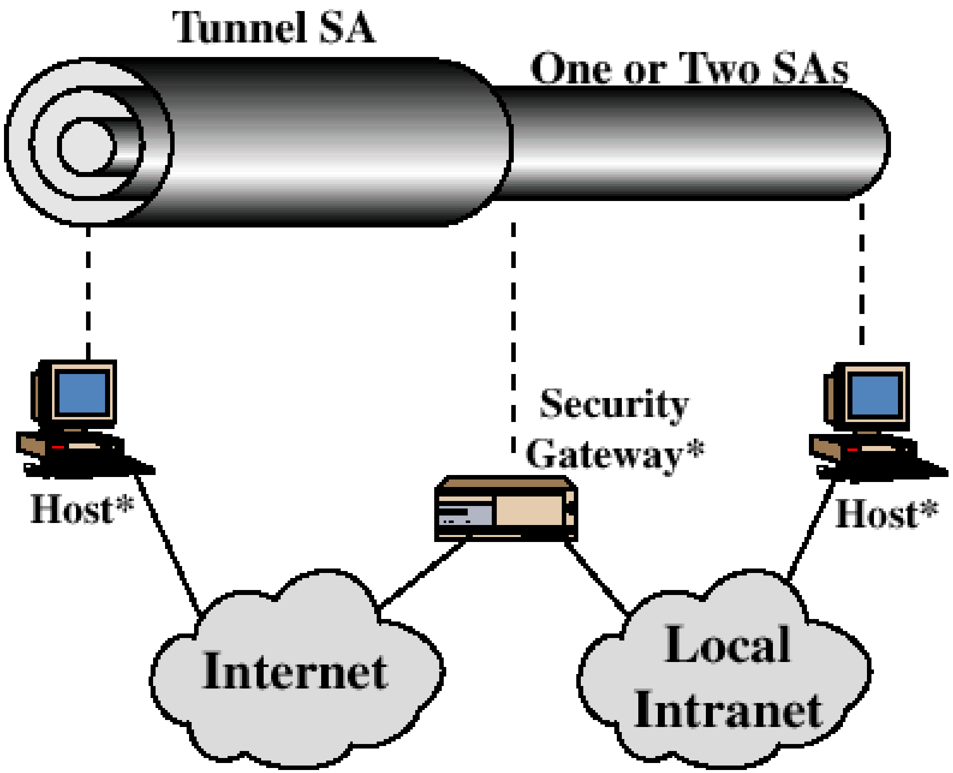
Combinations of Security Associations



(c) Case 3

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

Combinations of Security Associations



(d) Case 4

http://sce.uhcl.edu/yang/teaching/......
/IPsecurity.ppt

Key Management

- Two types:
  - Manual

    Problem: poor scalability
  - Automated
    - Internet Key Exchange, IKE

Evoluation of IKE

(source: https://www.rfc-editor.org/rfc/pdfrfc/rfc7296.txt.pdf)

- **IKEv1** was defined in RFCs 2407 [DOI], 2408 [ISAKMP], and 2409 [IKEV1].

  Internet Security Association and Key Management Protocol (ISAKMP)

  + Key Determination Protocols (Oakley, SKEME)

- **IKEv2** (RFC 4306) replaced all of those RFCs in IKEv1, and was clarified in [Clarif] (RFC 4718).
- RFC 5996 replaced and updated RFCs 4306 and 4718.

  Note: IKEv2 as stated in RFC 4306 was a change to the IKE protocol that was not backward compatible. RFC 5996 revised RFC 4306 to provide a clarification of IKEv2, making minimal changes to the IKEv2 protocol.

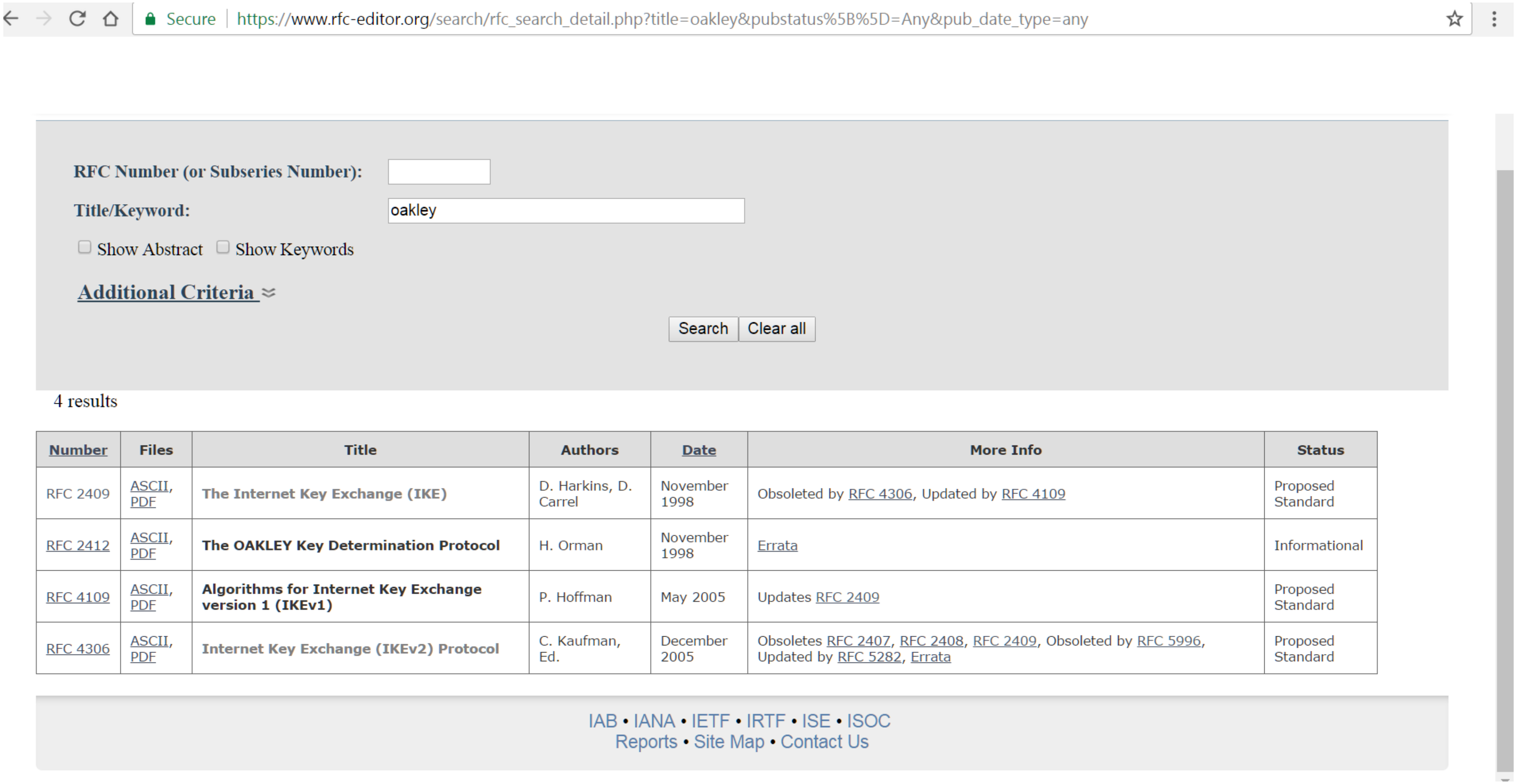
- RFC 7296 replaces RFC 5996.

Oakley

- Three authentication methods:
  - Digital signatures
  - Public-key encryption
  - Symmetric-key encryption (aka. Preshare key)

IETF documents/standards

- Use **RFC Editor** to find information and updates.



Secure https://www.rfc-editor.org/search/rfc_search_detail.php?title=oakley&pubstatus%5B%5D=Any&pub_date_type=any

RFC Number (or Subseries Number):

Title/Keyword: oakley

□ Show Abstract □ Show Keywords

Additional Criteria

Search | Clear all

4 results

Number	Files	Title	Authors	Date	More Info	Status
RFC 2409	ASCII, PDF	The Internet Key Exchange (IKE)	D. Harkins, D. Carrel	November 1998	Obsoleted by RFC 4306, Updated by RFC 4109	Proposed Standard
RFC 2412	ASCII, PDF	The OAKLEY Key Determination Protocol	H. Orman	November 1998	Errata	Informational
RFC 4109	ASCII, PDF	Algorithms for Internet Key Exchange version 1 (IKEv1)	P. Hoffman	May 2005	Updates RFC 2409	Proposed Standard
RFC 4306	ASCII, PDF	Internet Key Exchange (IKEv2) Protocol	C. Kaufman, Ed.	December 2005	Obsoletes RFC 2407, RFC 2408, RFC 2409, Obsoleted by RFC 5996, Updated by RFC 5282, Errata	Proposed Standard

IAB • IANA • IETF • IRTF • ISE • ISOC
Reports • Site Map • Contact Us

Internet Key Exchange

- Current standard: RFC 7296

  Internet Key Exchange Protocol Version 2 (IKEv2), OCTOBER 2014

- Exercises
  - **EX1:** Study the evolution of the Internet Key Exchange (IKE) protocol and draw a tree to highlight the changes (years, RFCs, etc.)

Internet Key Exchange

- Exercises
  - **EX2:** Study RFC 2409 to learn the authentication method based on digital signatures. Explain how that method works.
  - **EX3:** Study RFC 2409 and explain what '**Perfect Forward Secrecy**' is, and how that requirement would be met in the design of a security protocol.

Internet Key Exchange

- Exercises
  - **EX4:** Explain what ‘phase 1’ means in IKEv1. In IKEv2, what specific exchanges represent that phase?
  - **EX5:** Explain what ‘phase 2’ means in IKEv1. In IKEv2, what specific exchange(s) represent that phase?

Internet Key Exchange

- Exercises
  - **EX6:**
  - **EX7:**

Recommended Reading

- Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols and Architecture*. Prentic Hall, 1995
- Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley, 1994