IPSec contents

- IPSec overview, IPSec modes: Jani Koski
- SA, SPD, IPSec Policy: Heidi Lagerström
- AH, ESP, encrypting/decrypting: Jatta Rantala
- IKE: Ville Wettenhovi

IPSec, *background*

- IPSec is security feature implemented in the IP level
- IPSec Standard:
  - Standard developed by the IETF (Internet Engineering Task Force) since 1992
  - First version in 1995
  - Improved version (including IKE) in 1998
  - Still being developed at the IETF (e.g IKEv2)
- Good IPSec sources:
  - http://www.ietf.org/html.charters/ipsec-charter.html
  - book: Doraswamy, N., and Harkins, D. *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Prentice Hall, 1999.

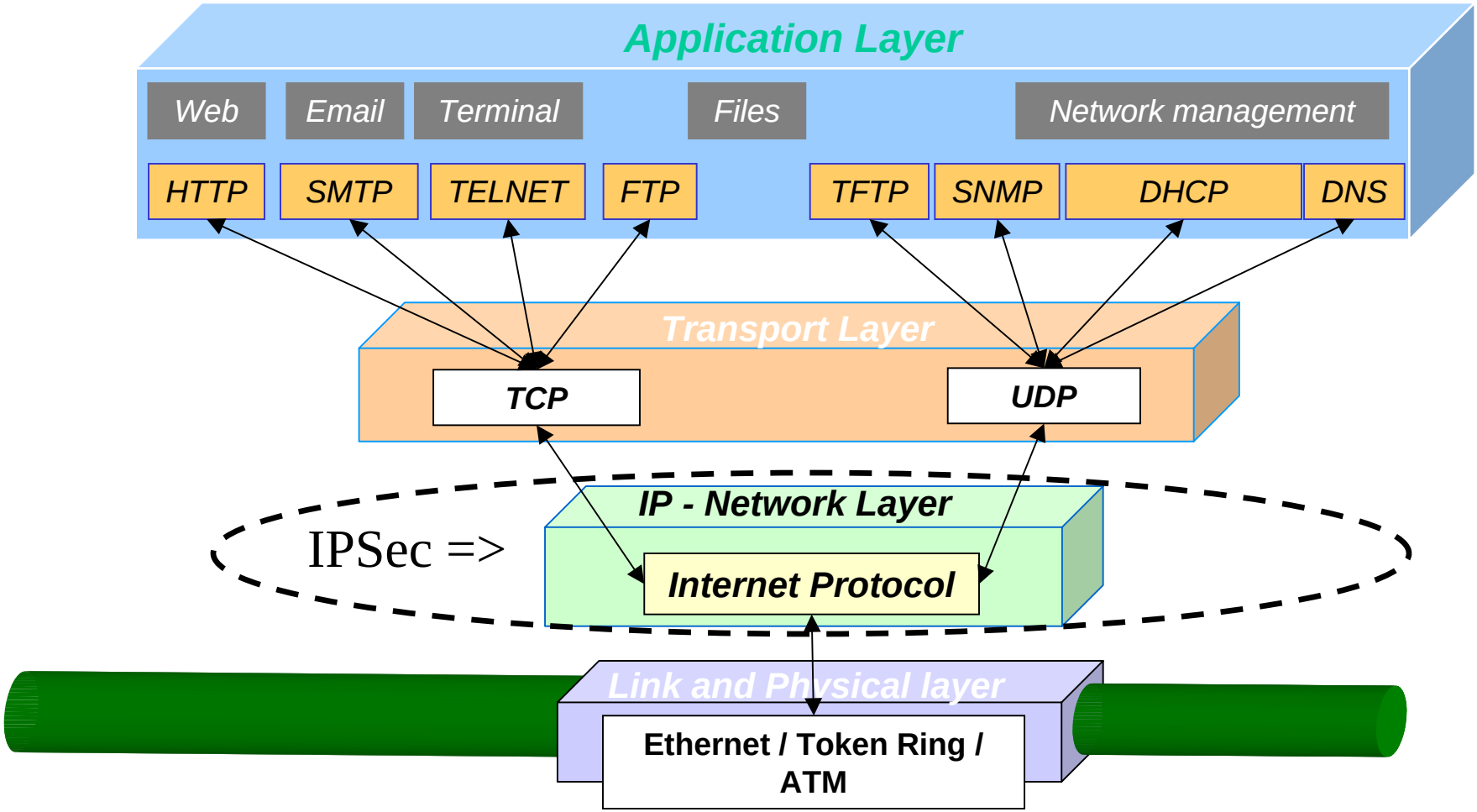
IPSec: *Advantages and Limitations*

- Advantages
  - Rather complete system which can provide numerous security services
  - Transparently provides network security for all applications
  - Standard => ensures interoperability between vendors
  - Scaleable to big networks
- Limitations
  - Complex, still evolving
  - No centralized and dynamic mgmt system for security policies
  - Full support for PKI is a challenging task for IPSec vendors
  - Certificate handling with IKEv1 is complex. IKEv2 possibly solves the problem.

Attacks and Protection in Internet

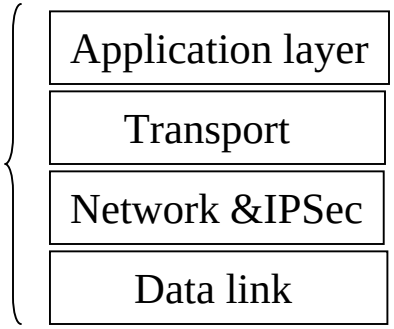
- some example attacks in Internet:
  - Denial-of-service
  - Eavesdropping
  - IP-spoofing
- Securing the Internet traffic can be implemented by several means:
  - Application specific security (e.g. e-Mails protected by PGP)
  - Transport layer (e.g. TLS, SSL)
  - Network level protection (e.g. IPSec)
    - Application independent
    - Scaleable to big networks
    - Transparent to the end-user
  - Link level security
    - Costly to implement

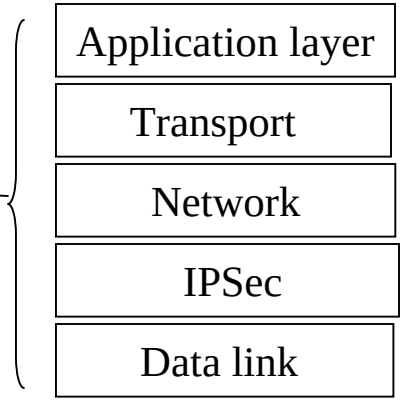
TCP/IP stack layer

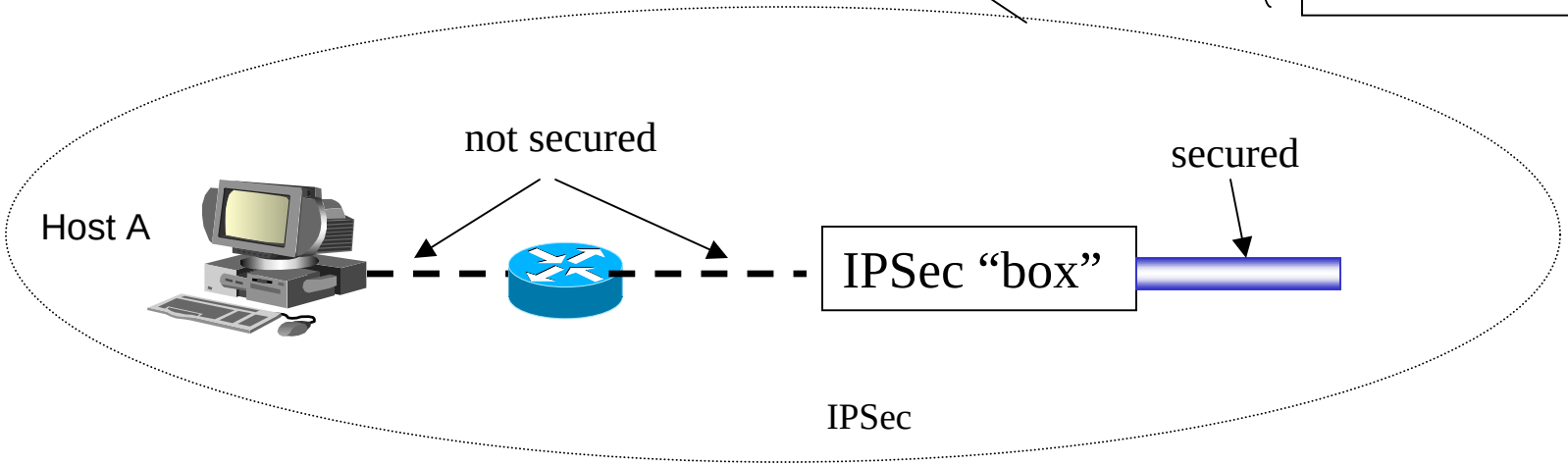


IPSec implementation

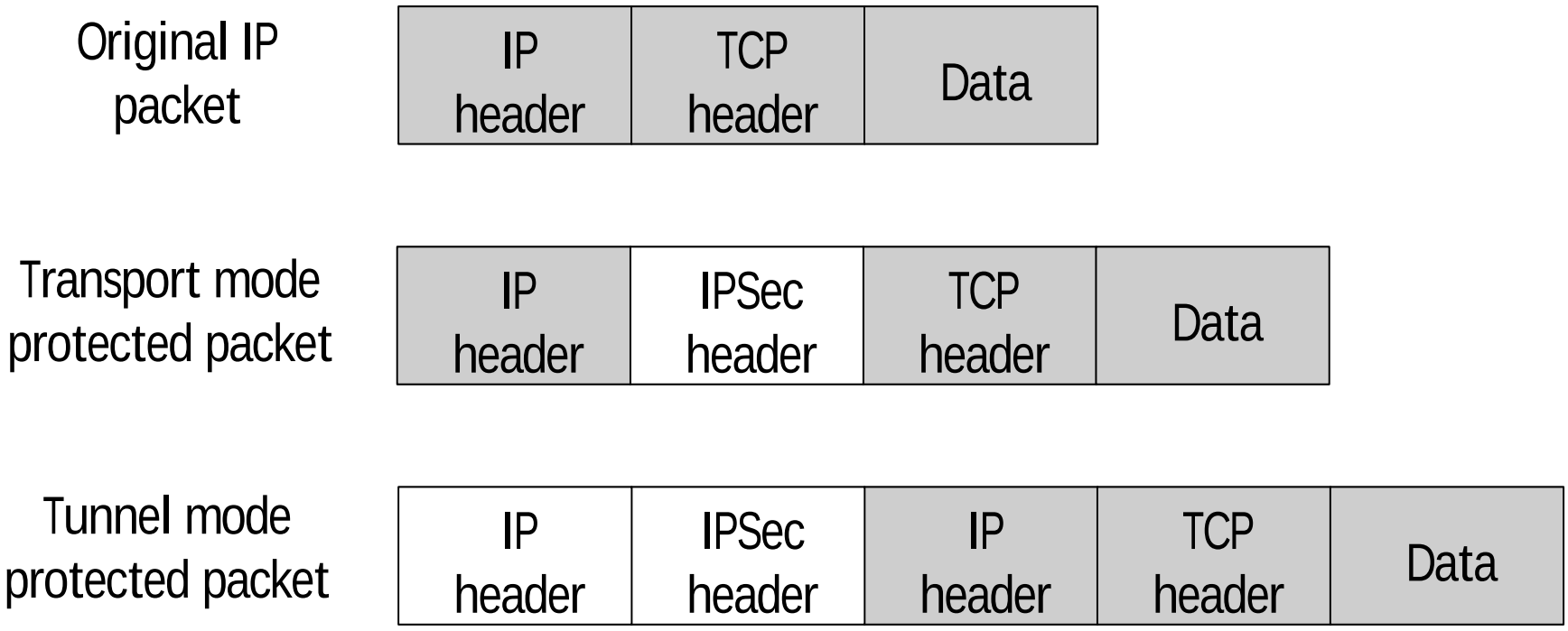
- IPSec can be implemented to:
  - End hosts
  - Gateways
  - Routers
- OS integration:
- BITS (Bump In The Stack):
- BITW (Bump In The Wire):







IPSec modes: transport & tunnel

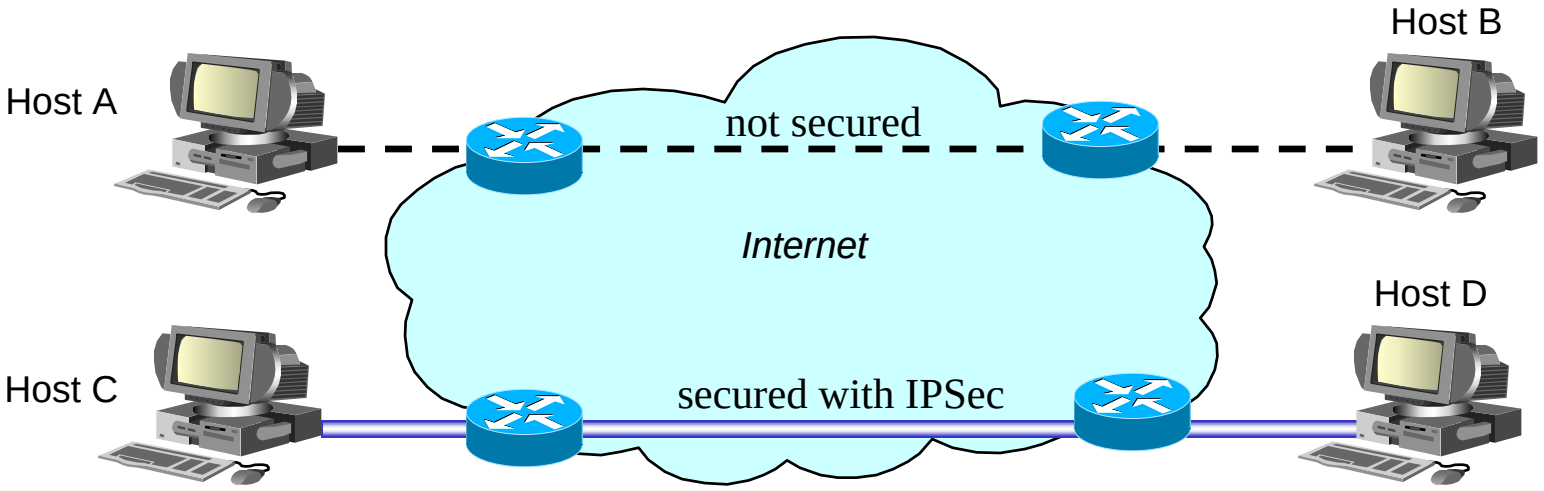


Transport mode - the transport layer packet (typically TCP) is encapsulated in IPSec. Communication endpoint equals to cryptographic endpoint.

Tunnel mode – the whole IP packet is encapsulated. Communication and cryptographic endpoints may be different.

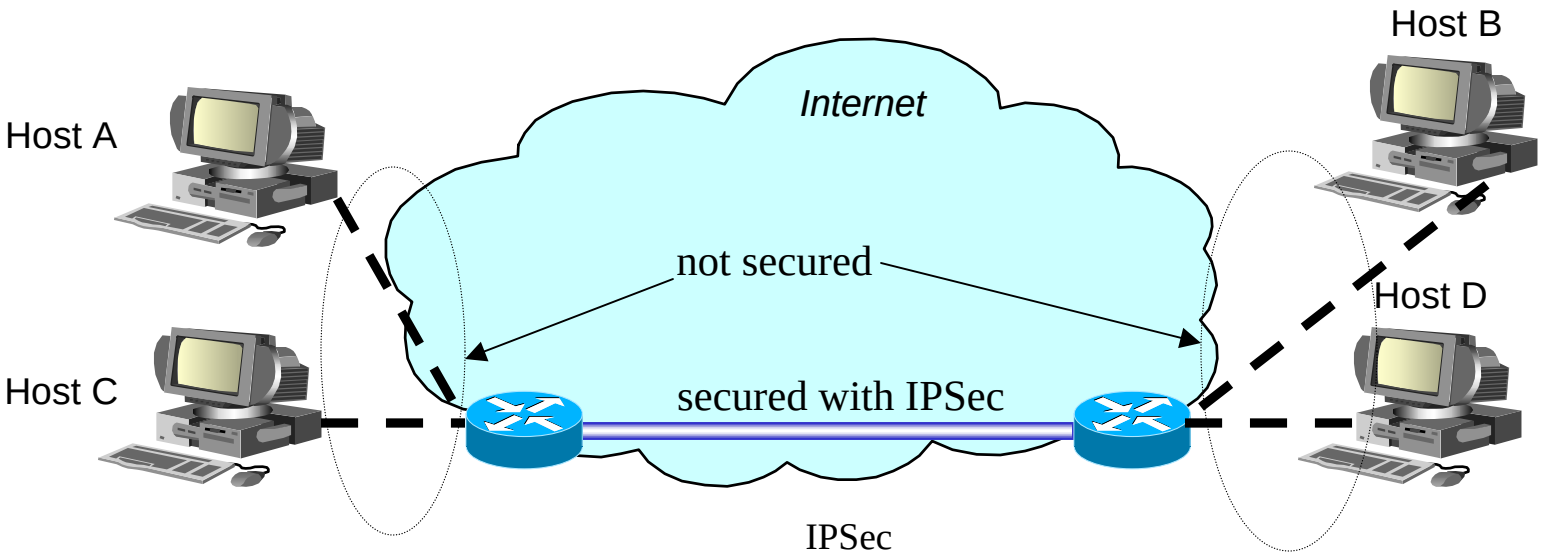
IPSec transport mode

- Transport mode
  - AH and ESP protects the transport header
  - Security provided by the hosts (host-to-host security)
  - Provides configured security
  - IPsec must be implemented at both end-points



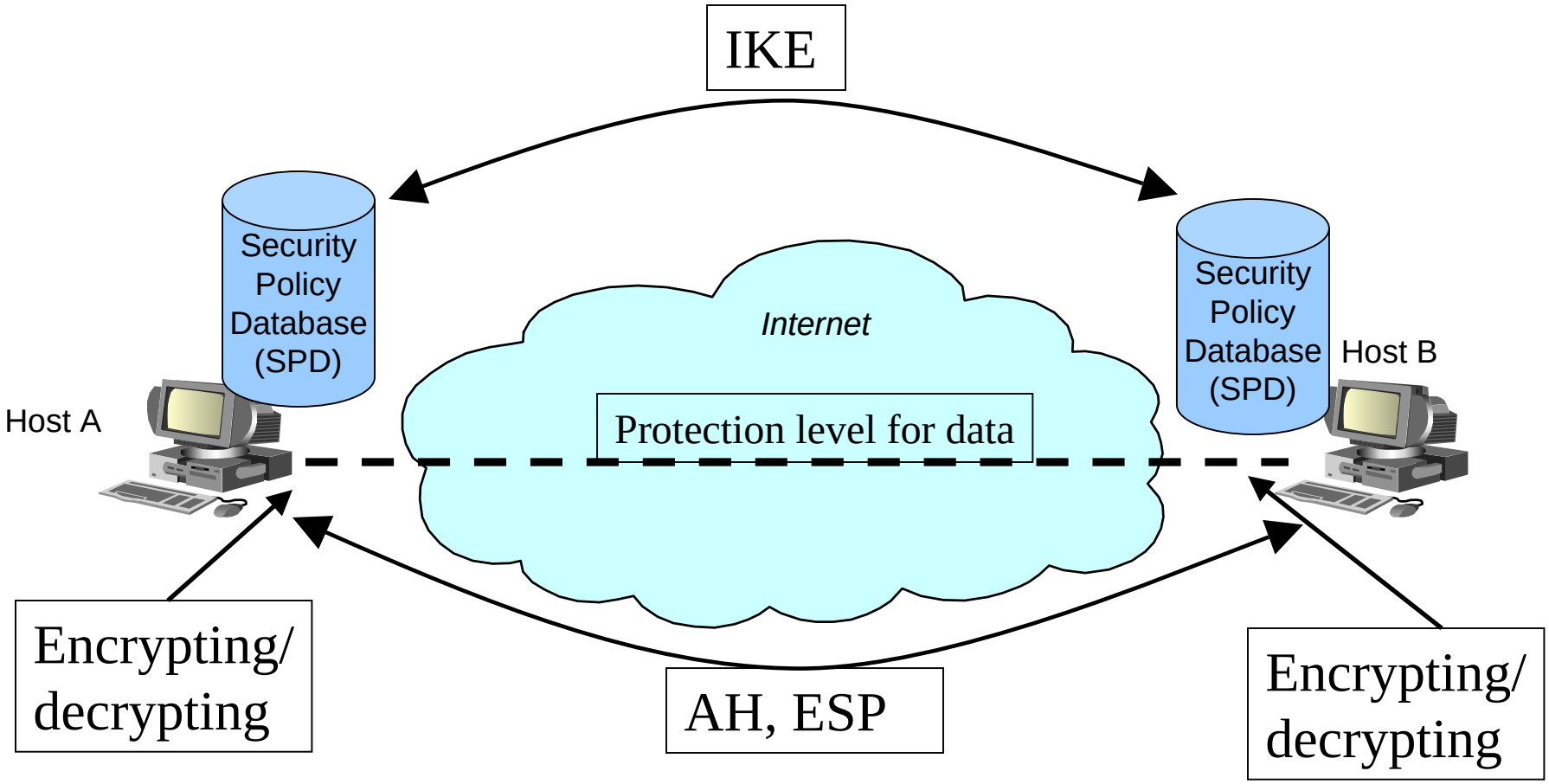
IPSec tunnel mode

- Tunnel mode:
  - Security provided by other devices (e.g. routers) than hosts => no need to install IPSec to every host (e.g. in in corporate with e.g. 200 computers)
  - VPN application, internal IP addresses not visible externally



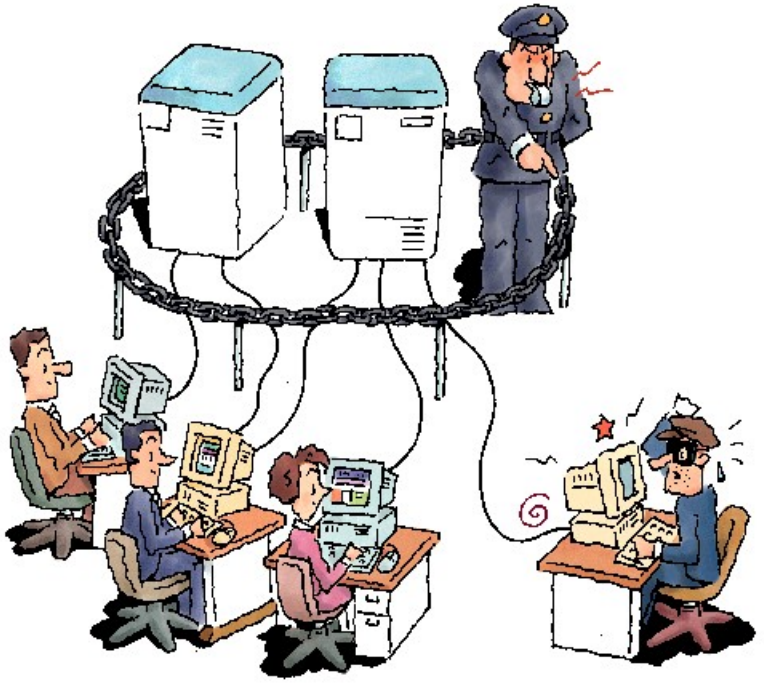
SA, SAD, SPD, AH, ESP, IKE?

- what actually happens there when IPSec is used?

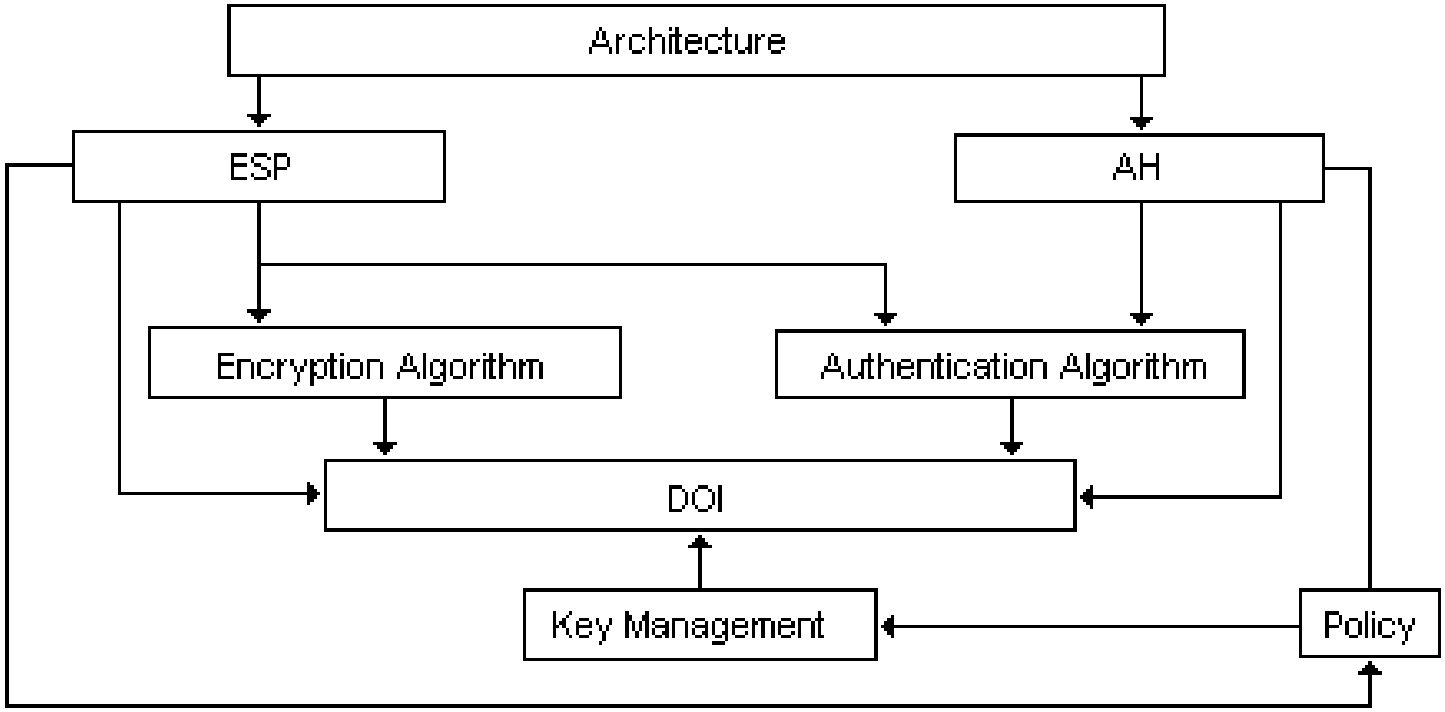


IPSec: Part II
Heidi Lagerström

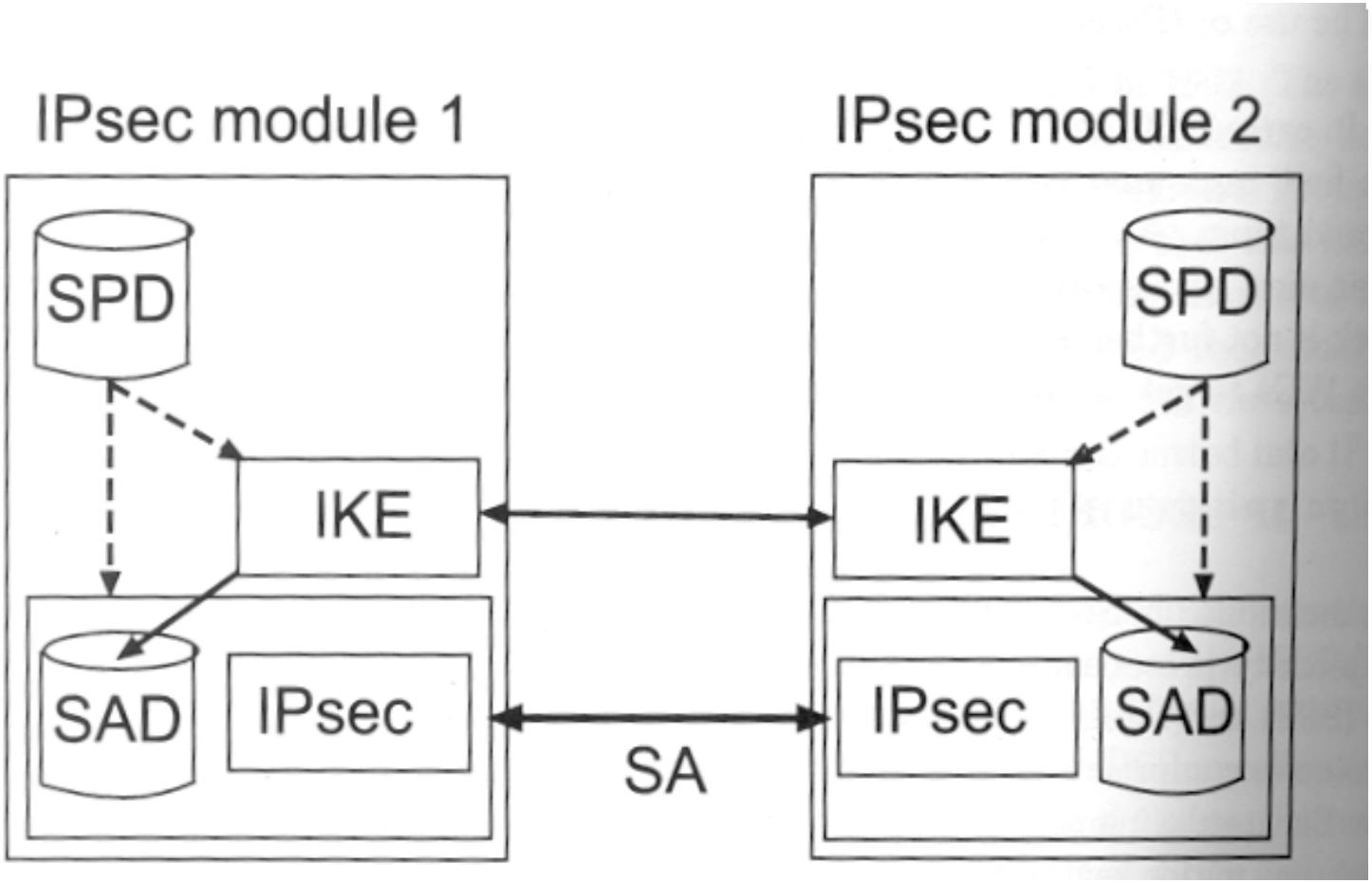
- IPSec Architecture
- Security Association (SA)
- Databases (SAD, SPD)
- IPSec Policy
- IPSec packet processing



IPSec Roadmap

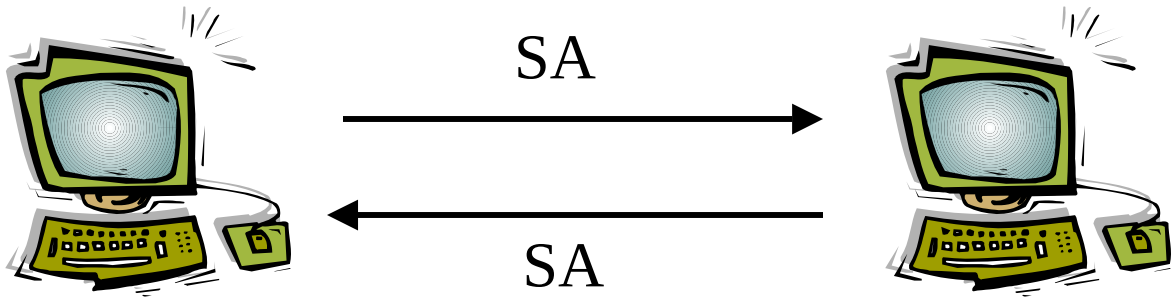


IP Security Architecture



Security Association (SA)

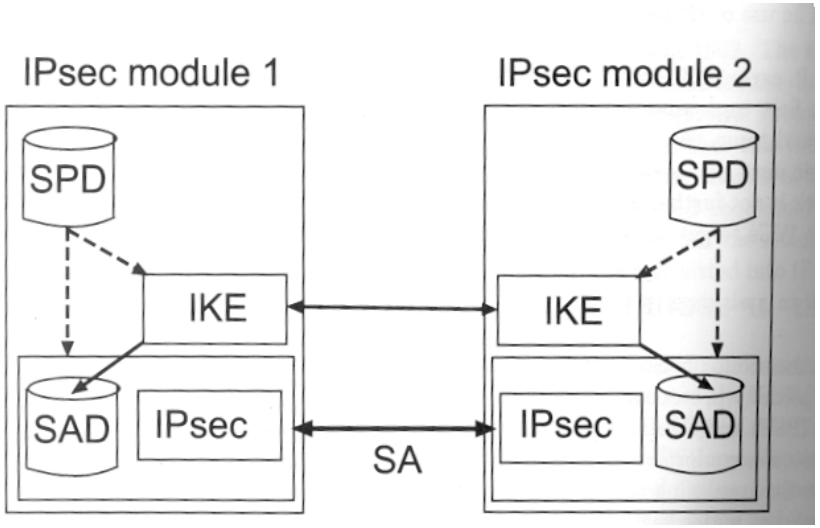
- SA is a contract between communicating parties
- Describes how the entities will use security services to communicate securely
- Uses AH or ESP security protocol
- Unidirectional



Creation of SA

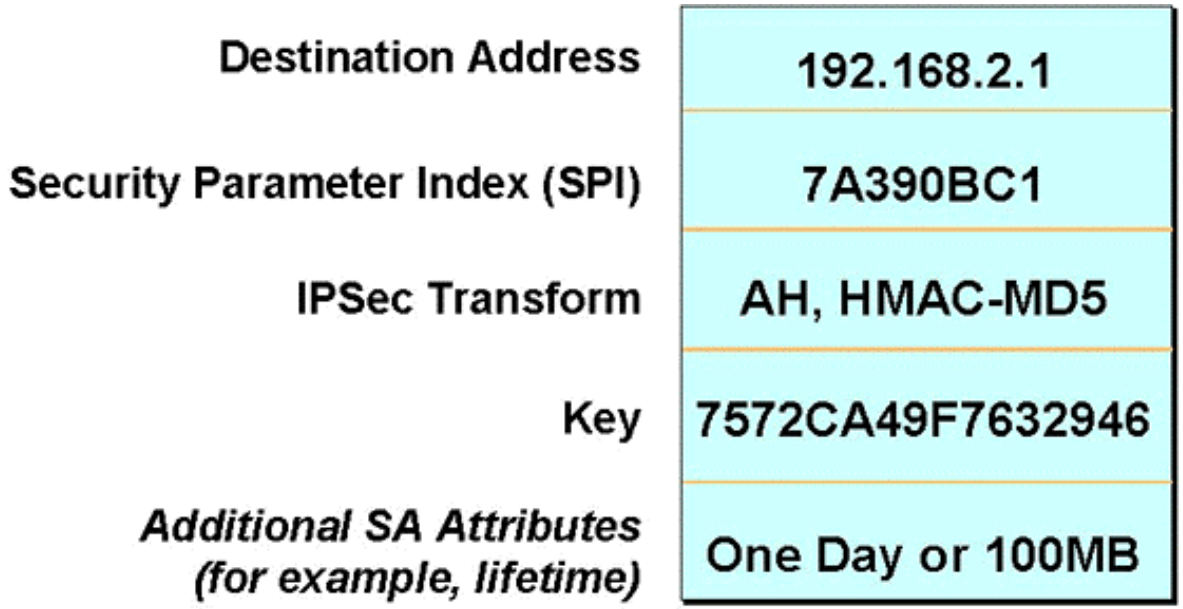
- Manually

- Through IKE

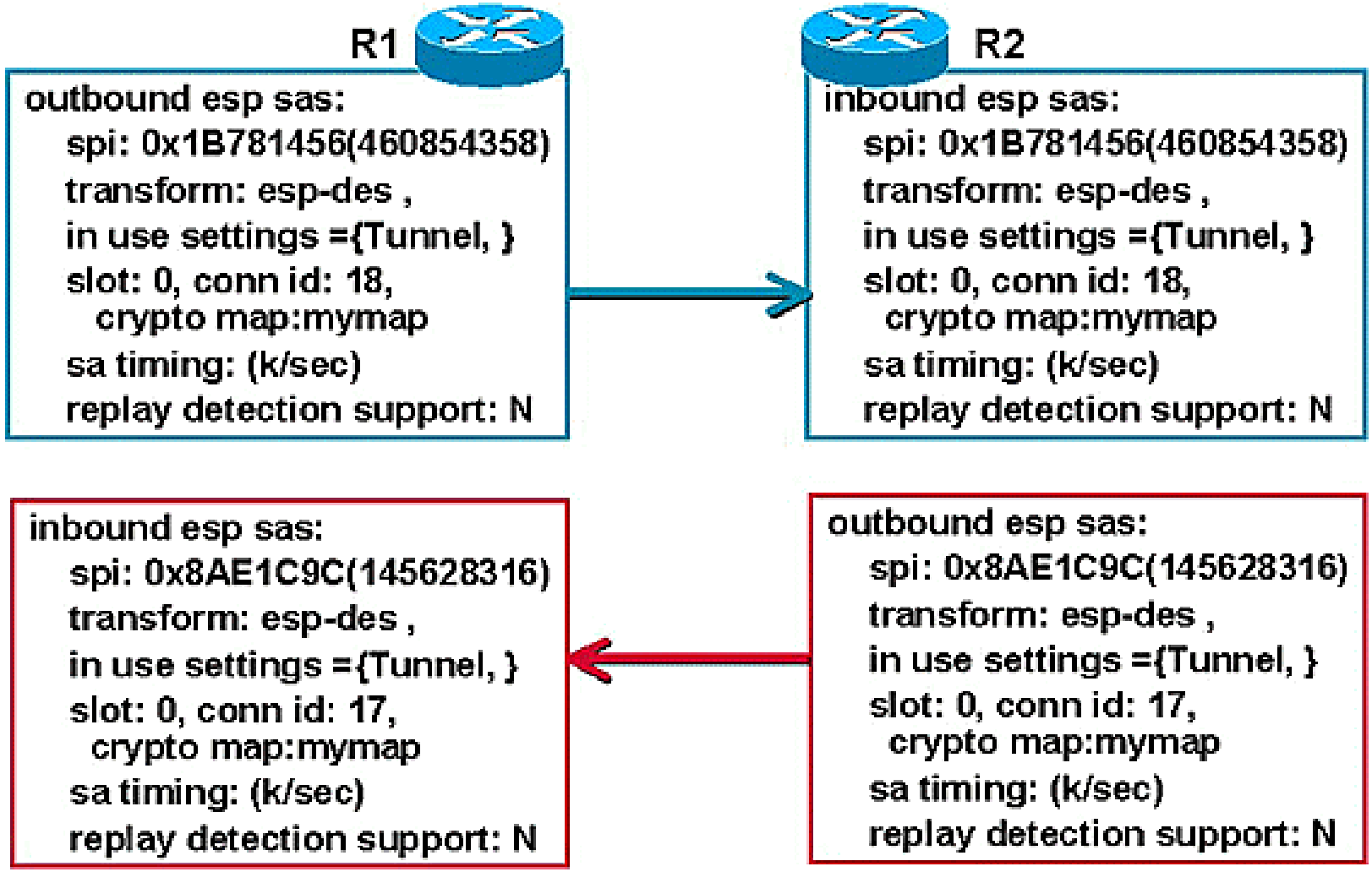


SA is deleted if
1) lifetime has expired
2) the keys are compromised
3) the number of bytes has reached a threshold
4) other end requests it

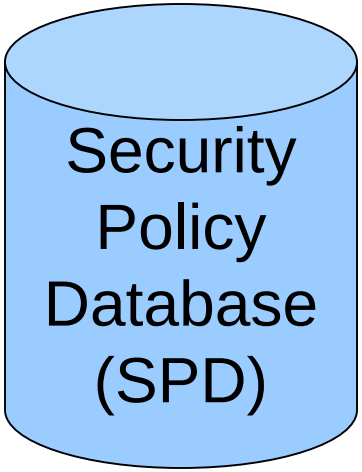
Security Association Structure



SA parameter example



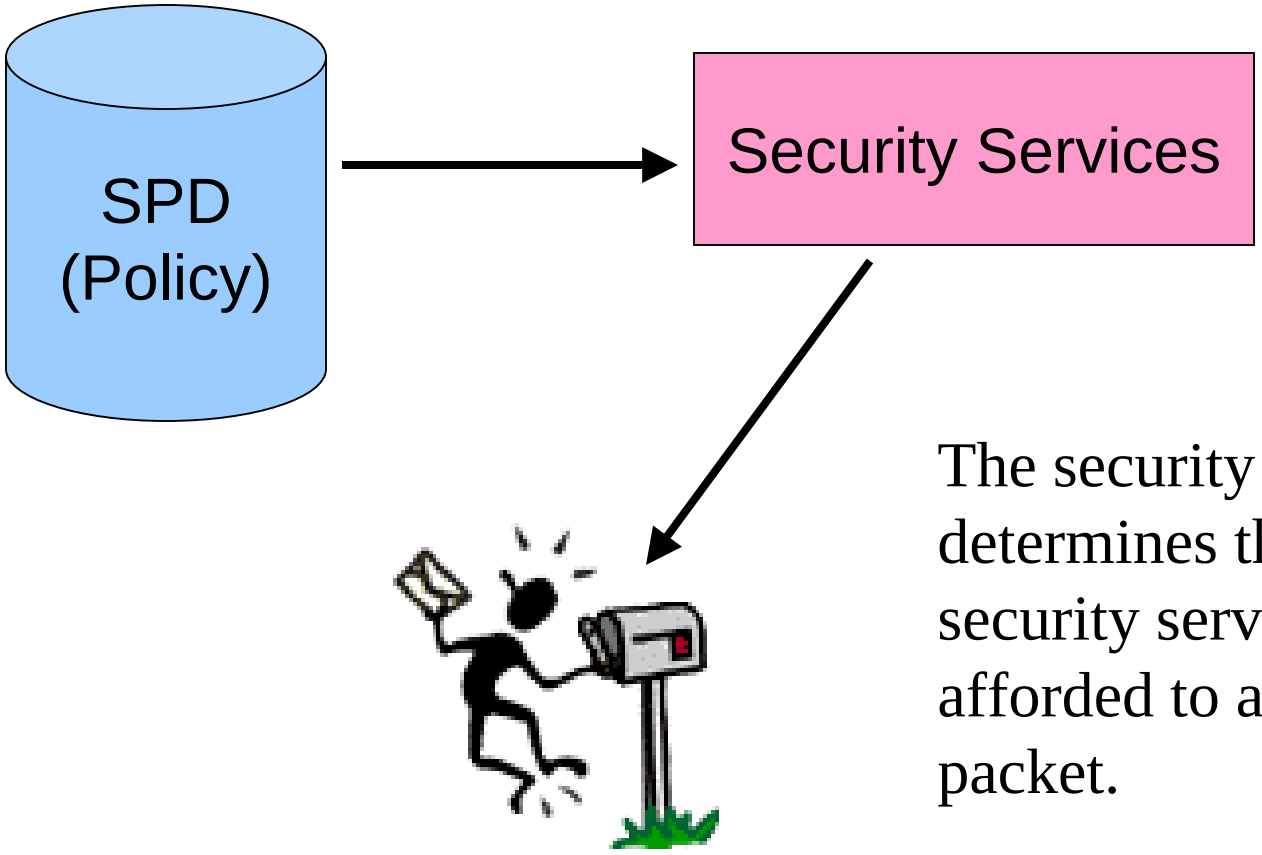
Security Association Databases



• Specifies the policies that determine the disposition of all IP traffic

• Contains parameters that are associated with each (active) security association

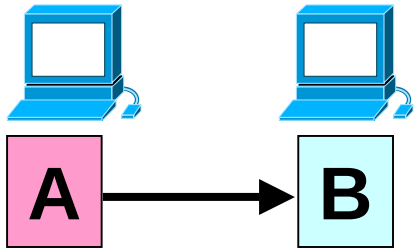
IPSec Policy



The security policy determines the security services afforded to a packet.

Outbound Processing

Outbound packet (on A)



IP Packet

Is it for IPSec?
If so, which policy entry to select?

SPD
(Policy)

SA
Database

…

…

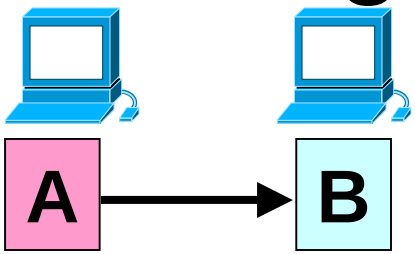
Determine the SA and its SPI

IPSec processing

SPI & IPSec Packet

Send to B

Inbound Processing



Inbound packet (on B)

From A

SPI & Packet

SA Database

Use SPI to index the SAD

…

"un-process"

SPD (Policy)

…

Was packet properly secured?

Original IP Packet

IPSec: Part III
Jatta Rantala

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)
- Authentication algorithm (MD5)
- Encryption algorithm (DES-CBC)

Sources:

- Kaufman, Perlman, Speciner, **Network Security, Private Communication in a public world**, Prentice Hall, 2002, p. 423-439

-Peterson, Davie, **Computer Networks, A Systems approach**, 2nd edition, Morgan Kaufmann, 2000, p. 605-608

- A cryptographic evaluation of IPSec, Neil Ferguson and Bruce Schneier, http://www.cs.wpi.edu/~rek/Adv_Nets/Spring2002/IPSec.pdf

- IPSec - Overview on current documents,

http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html

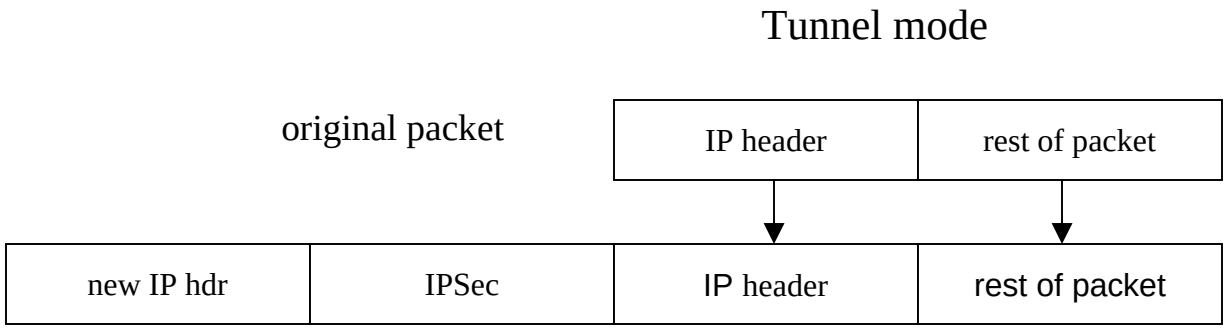
- IPSEC - Internet Protocol Security,

http://www.tcm.hut.fi/Tutkimus/IPSEC/chapter2.html

General about AH and ESP

- Two types of IPSec headers inserted into the IP packet that implement the available security services and tell to the recipient to which security association the packet belongs to
- AH provides access control, connectionless message integrity, authentication and antireplay protection
- ESP provides besides these confidentiality by encryption algorithms
- AH and ESP can be used by themselves or together to provide the mix of services the user wants
- Given that ESP optionally provides integrity protection is AH needed?

• Integrity protection provided by ESP and AH are not identical => AH provides integrity protection for some of the fields inside th IP header as well => Why protect the IP header?



• With ESP everything beyond the header is encrypted => routers and firewalls are not able to look at some fields such as layer 4 ports => Good thing according to security advocates, because fields such as TCP ports should be hidden to avoid divulging information

• According to authors of the book **Network Security, private communication in a public world** AH is not needed as will be argued later

AH (Authentication Header)

- Defined in RFC 2402, http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/RFCs/rfc2402.txt
- Provides connectionless integrity and data origin authentication for IP datagrams (not encryption)
- Optionally provides protection against replays
- AH header either follows IPv4 header or is an IPv6 extension header, depending on which version of IP it is used with

# octets	
1	next header
1	payload length
2	unused
4	SPI (Security Parameter Index)
4	sequence number
variable	authentication data

Mutable, Immutable

- Some fields in the IP header get modified by the routers => can’t be included in AH’s end-to-end integrity check
- Immutable fields = fields that AH designers do not believe should ever legitimately be modified in transit
- IPv4 mutable fields: TYPE OF SERVICE, FLAGS, FRAGMENT OFFSET, TIME TO LIVE, HEADER CHECKSUM
- IPv6 mutable fields : TYPE OF SERVICE, FLOW LABEL, HOP LIMIT
- Fields that are *mutable but predictable* are included in the AH integrity check, but with the values they will have when received at the other end (e.g. DESTINATION ADDRESS in source routing)

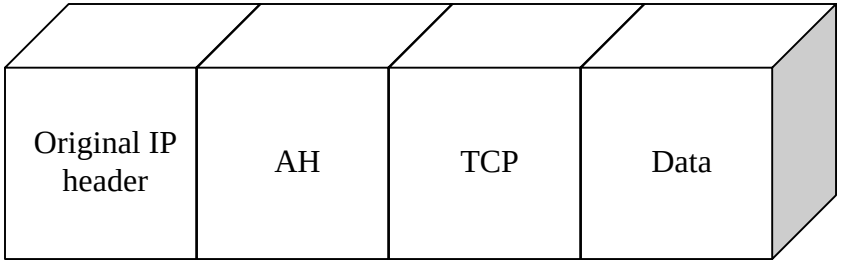
ESP (Encapsulating Security Payload)

- Allows for encryption and/or integrity protection
- Integrity protection only => ESP or AH
- Both encryption and integrity protection => both ESP and AH, or do both with ESP
- ESP always does encryption => if you don't want encryption use the special "null encryption" algorithm (RFC 2410)

# octets	
4	SPI (Security Parameters Index)
4	sequence number
variable	IV (initialization vector)
variable	data
variable	padding
1	padding length (in units of octets)
1	next header/protocol type
variable	authentication data

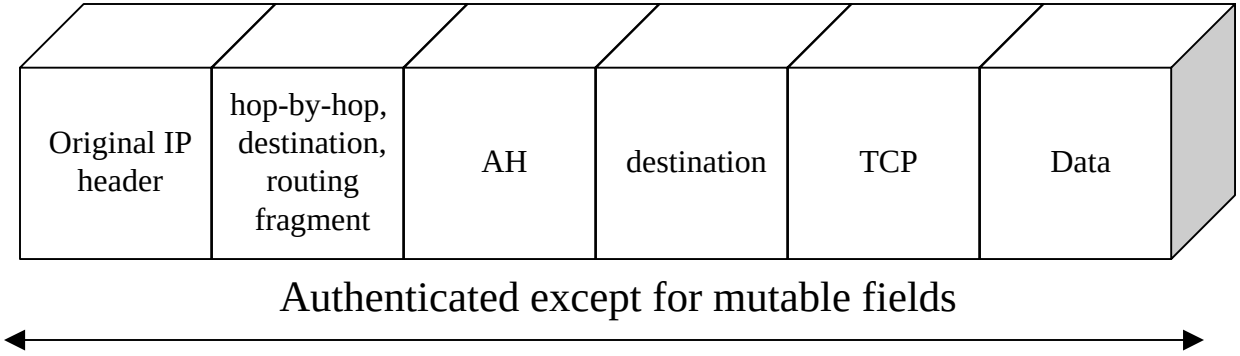
Transport mode AH

AH is stronger in this mode as it also authenticates some of the IP header fields.



IPv4

Authenticated except for mutable fields

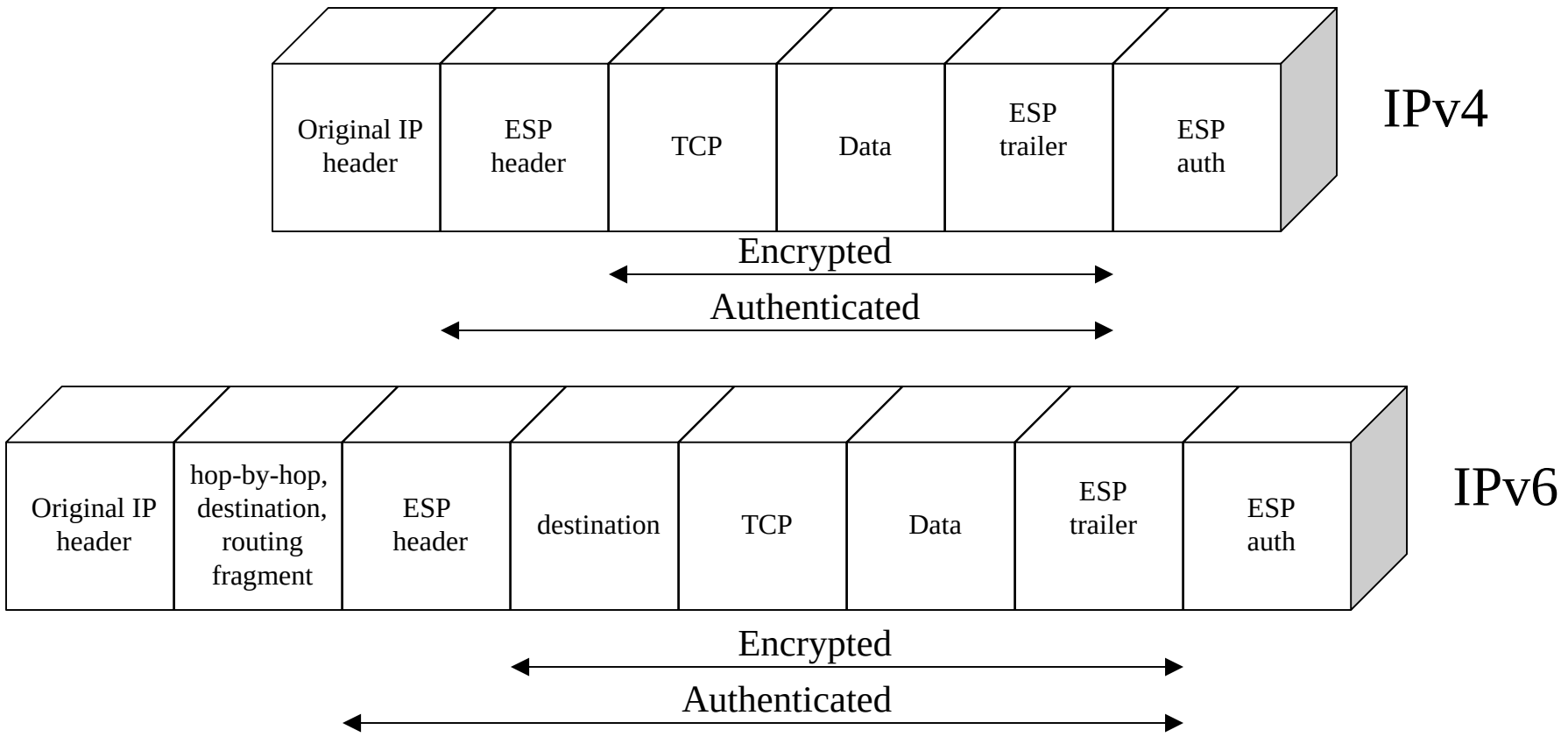


IPv6

Authenticated except for mutable fields

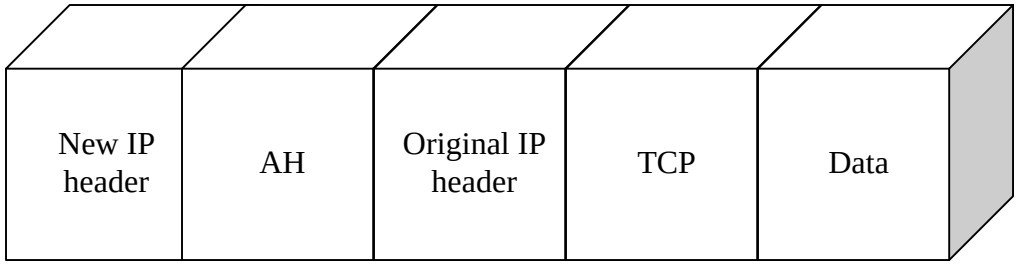
Transport mode ESP

ESP trailer is used for adding the padding and the NextHdr fields.
ESP Authentication is used when authentication is carried by ESP.



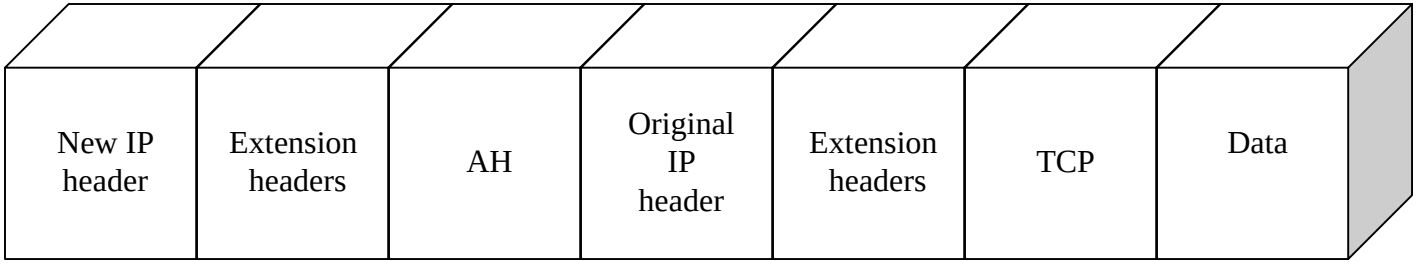
Tunnel mode AH

In tunnel mode the payload includes the original IP header.



IPv4

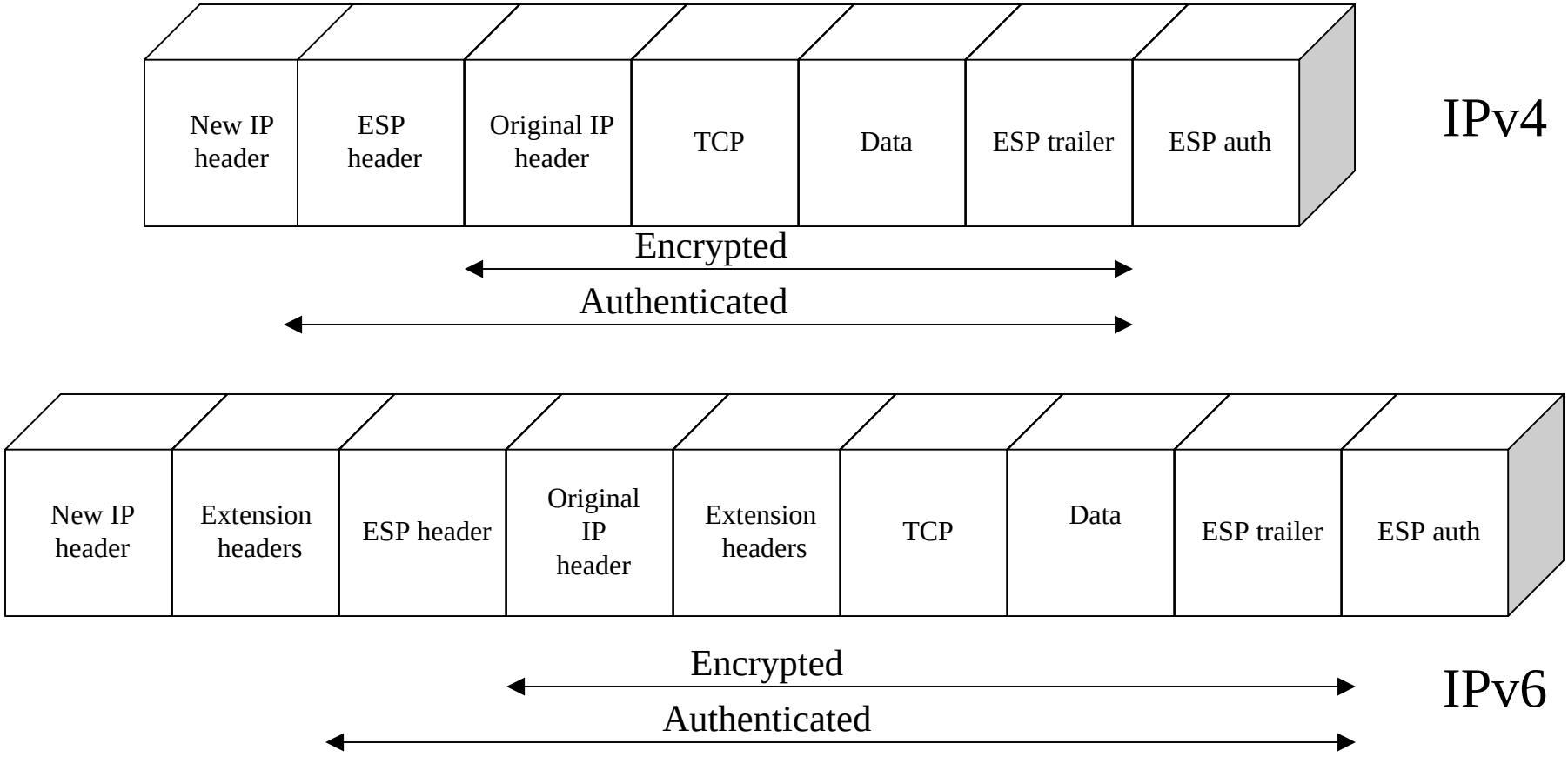
Authenticated except for mutable fields in the new IP header



IPv6

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

Tunnel mode ESP

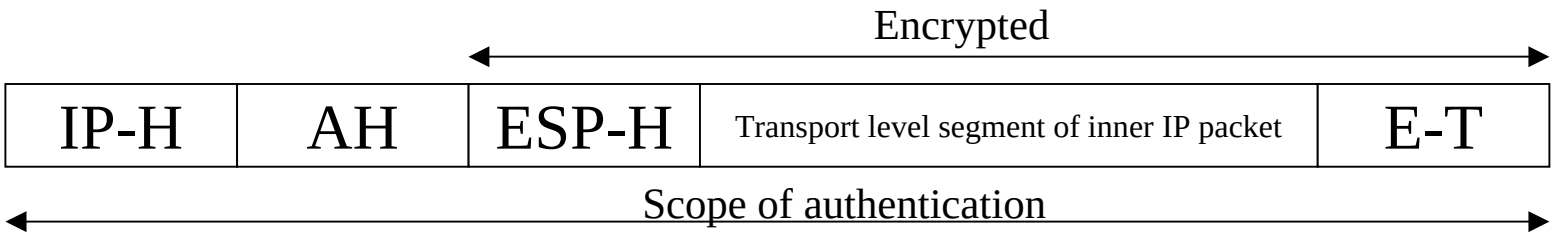


Encryption before/after authentication?

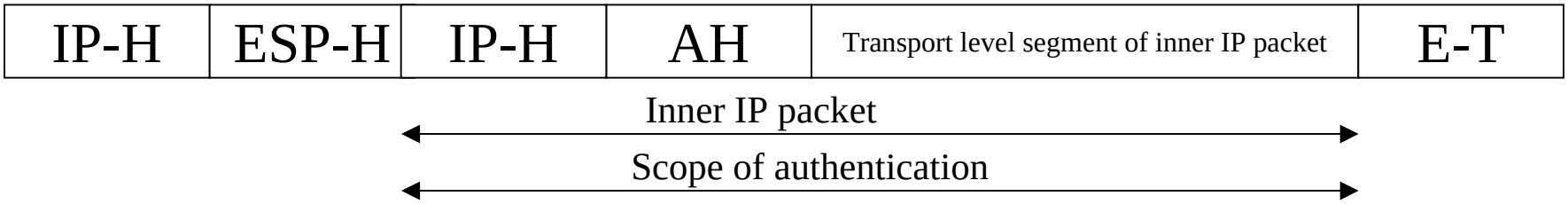
Advantages of applying authentication before encryption:

• Since AH is protected by ESP it is impossible for anyone to intercept the messages and alter the AH without detection

• If it is required to store the authentication information it is benefitial as the authentication information applies to plaintext message not cipher-text message



1) Encryption before authetication (tunnel/transport mode)



2) Authentication before encryption (tunnel mode)

So, do we need AH?

Reasons that people give for keeping AH:

- AH protects the IP header, whereas ESP only protects everything beyond the ESP header => protecting the IP header doesn't matter for security
- With ESP, even when not using encryption, firewalls and routers cannot look beyond the layer 3 header at information => routers and firewalls have no right to look at anything above layer 3; anything copied over in cleartext exposes some info that might better be hidden from eavesdroppers; since the IPSec key is end-to-end, it is impossible for intermediate devices to verify that the cleartext fields are accurate.
- An implementation that only implemented AH might be more exportable => even if an implementation of IPSec that only did AH were more exportable, it's not very important because who would by it?

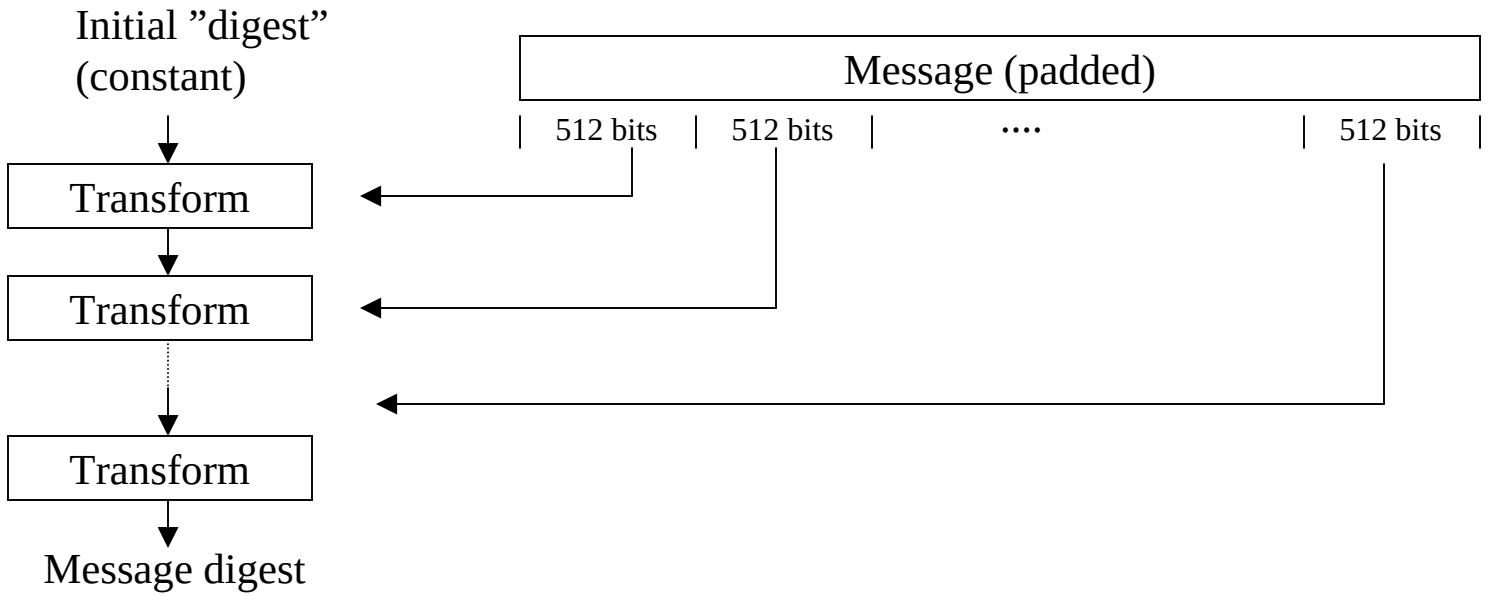
=> rather than seeing the feature of exposed layer 4 information as a reason to keep AH, IPSec should be considered as essentially always providing encryption and if the layer 4 information needs to be exposed, there will have to be a way to exposing it with ESP.

General about the algorithms used with IPSec

• The encryption and authentication algorithms are directly responsible for the strength the security the system can provide
• IPSEC must be able to balance between the legal restrictions in use of strong encryption and authentication, and the one that is available everywhere
• All hosts claiming to provide IPSEC services must implement the AH with at least the MD5 algorithm using a 128-bit key
• All ESP implementations must support the use of the Data Encryption Standard (DES) in Cipher-Block Chaining (CBC) mode
• Other cryptographic algorithms and modes may also be implemented in addition to this mandatory algorithm and mode, but MD5 and DES-CBC should be set as default algorithms.

MD5 (Message Digest 5)

- Computes a fixed-length cryptographic checksum from an arbitrary long input message
- Has some things in common with DES: they don’t have a formal mathematical foundation => rely on the complexity of the algorithm to produce a random output



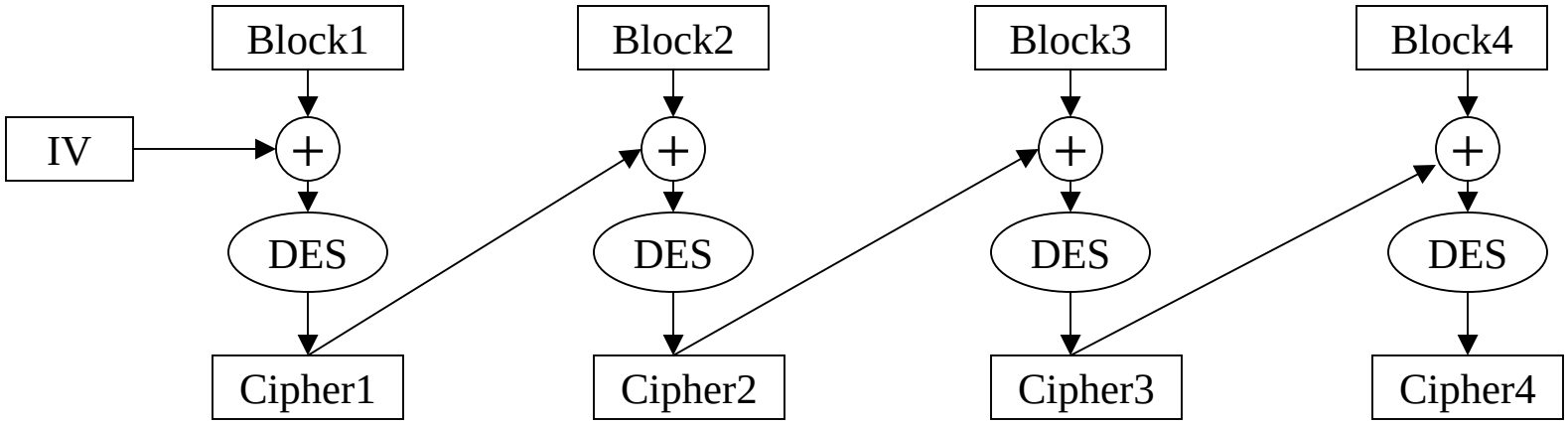
DES-CBC (Data Encryption Standard Cipher Block Chaining)

DES:

- Encrypts a 64-bit block of plaintext using a 64-bit key
- The 64 bits in the message block are permuted
- 16 rounds of identical operations are applied to the resulting data and the key
- The inverse of the original permutation is applied to the result

DES-CBC:

- To encrypt a longer message using DES CBC is used. The idea: The ciphertext for block i is XORed with the plaintext for block i+1 before running it through DES. An initialization vector IV is used for block 0.



IPSec: Part IV

Ville Wettenhovi

IKE
(Internet Key Exchange)

IKE overview

- SA can be created manually or automatically
- Internet Key Exchange (IKE) is automated protocol for SA management and exchange keys through public networks
- It is meant for establishing, negotiating, modifying and deleting SAs
- IKE is hybrid protocol. It integrates the Internet Security Association and Key Management Protocol (ISAKMP), Oakley and SKEME
- ISAKMP is a key exchange independent framework for authentication, SA management, and establishment
- Oakley defines series of key exchanges and services provided each. Oakley is used in phase one, creation of SA
- SKEME defines a exchange which provides anonymity and fast key refreshment.

IKE overview

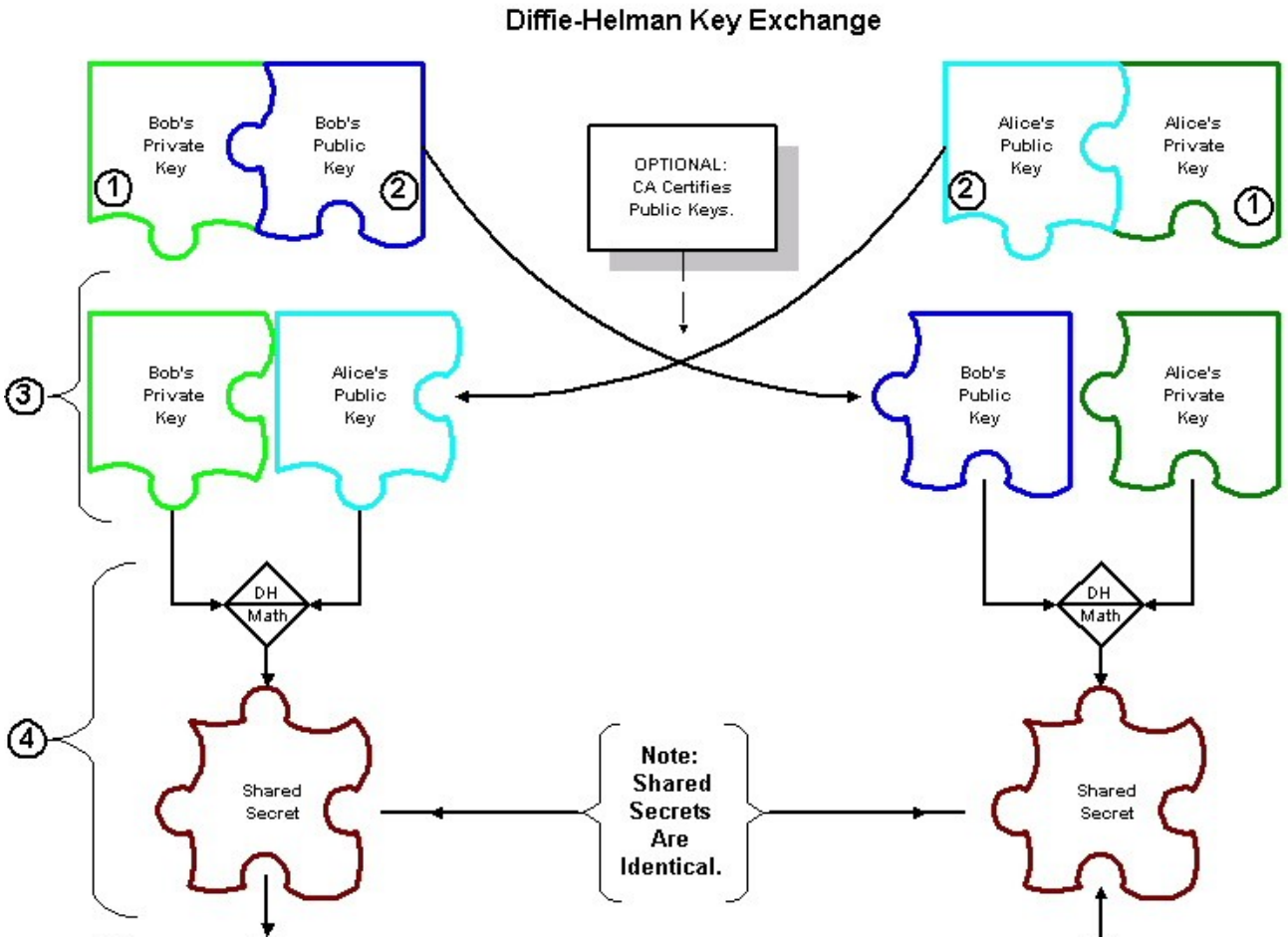
- IKE uses (normally) the UDP port 500
- DOI (Domain of Interpretation) defines how to use IKE.
- IKE is defined by RFC 2409

IKE provides a way to:

- Ensure that the key exchange and the IPSec communication you are about to begin take place between authenticated parties
- Negotiate the protocols, algorithms and keying material to be used between two IPSec peers
- Update and re-negotiate SA securely after they have expired

Diffie-Hellman key exchange

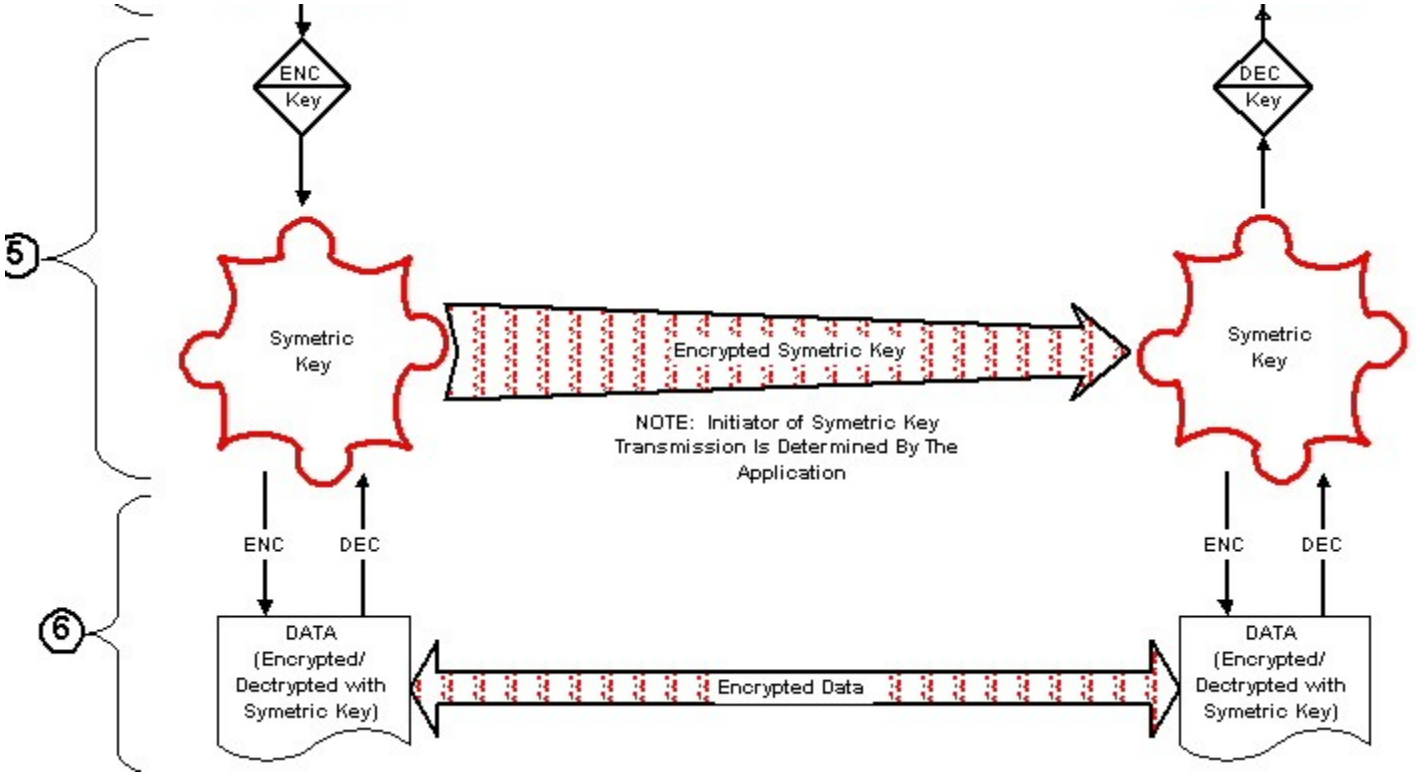
- IKE uses a scheme called Diffie-Hellman for key exchange
- It was developed by Whitfield Diffie and Martin Hellman in 1976
- Both peers generates their own public/private key pair. Each send public key to other
- Each then combines the public key they received with their own private key. The resulting value a ”Shared secret" is the same on both sides
- The shared secret then encrypts the symmetric key for secure transmit



1&2. Public/Private key pair is generated

3. Public key is transferred to another party

4. Shared secret is generated



5. Shared secret encrypt a symmetric key and transmit it
6. Data encryption and secure communication can occur

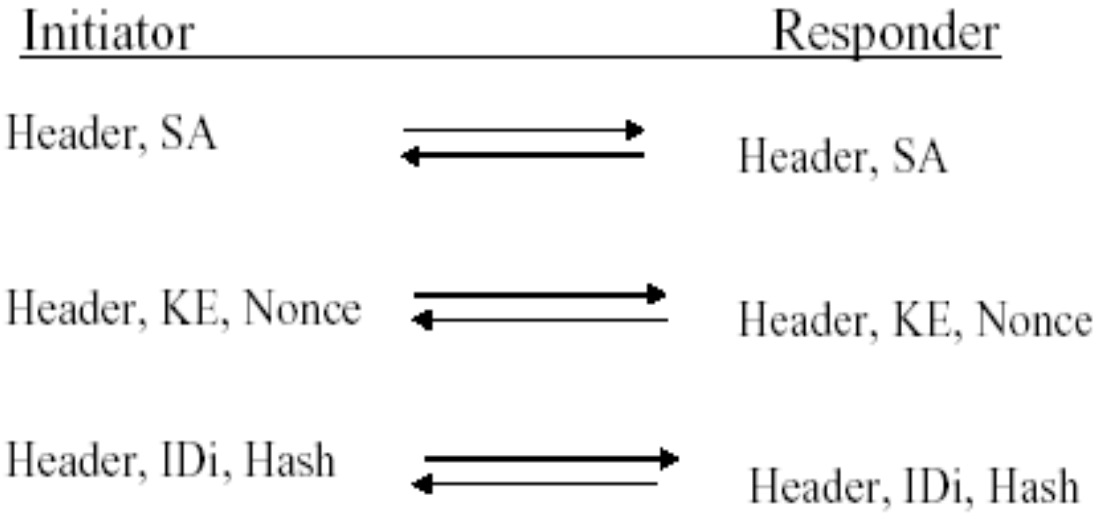
IKE phases

- IKE supports two phases
- In phase one, two peers establish a secure channel for doing IKE
- **Main mode** accomplishes a phase one exchange by establishing a secure channel
- **Aggressive mode** is another way of accomplishing a phase one exchange
- **Quick mode** accomplishes a phase two exchange by negotiating an SA for general purpose communications

IKE Main mode

- A mechanism for establishing the first phase IKE SA (Security Association)
- To agree authentication, algorithms, hashes and keys
- Main mode occurs in three two-way exchanges between the SA initiator and the responder
- After Main mode is established, phase 2 is performed to complete SA

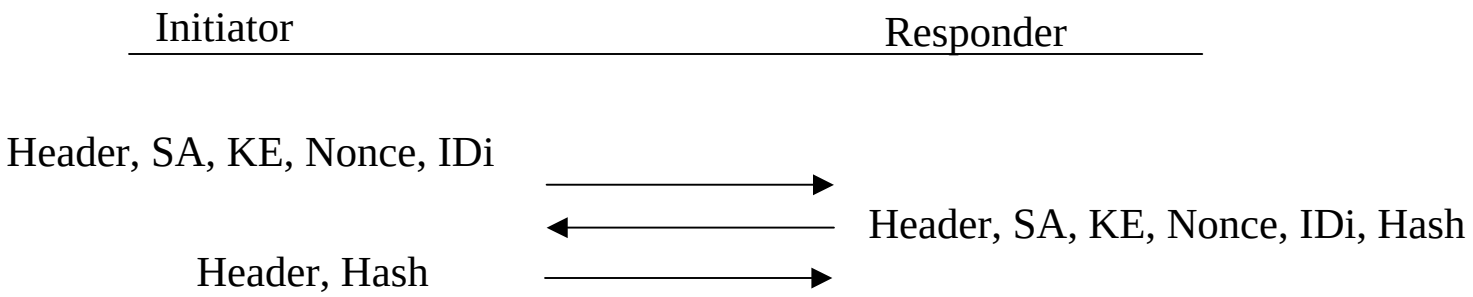
IKE Main mode



SA=Security Association, KE=Key Exchange, Nonce=random number, IDi= identity of the peer

- In the first exchange, peers agree on basic algorithms and hashes
- In the second section they exchange public keys for a Diffie-Hellman
- In the third section they verify those identities

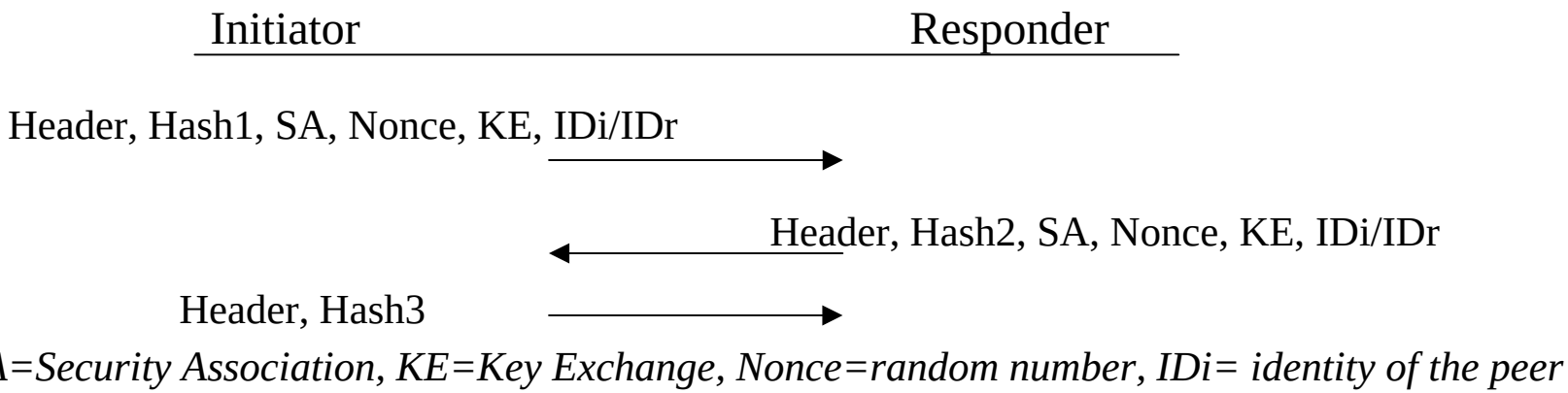
IKE Aggressive mode



SA=Security Association, KE=Key Exchange, Nonce=random number, IDi= identity of the peer

- Aggressive mode is more simple than the Main mode,
  In the aggressive mode there are only three messages exchanged
- Aggressive Mode is a bit faster, but it doesn't provide an identity protection
- The initiator offers a list of protection suites, his Diffie-Hellman public key value, his nonce and his identity.
- The responder replies with a selected protection suite, his Diffie-Hellman public value, his nonce, his identity and authentication payload, like a signature.

IKE Quick mode



SA=Security Association, KE=Key Exchange, Nonce=random number, IDi= identity of the peer

- Once two parties have established an IKE SA using Aggressive or Main mode they can use Quick mode
- Quick mode has two purposes: negotiating general IPSec services and generating fresh keying material
- Quick mode packets are always encrypted and always started with a hash payload

IKE Authentication Methods

- In the first part of the IKE exchange, an authentication method is agreed
- Four different authentication methods are allowed with the Main Mode and Aggressive Mode
- Authentication with Digital Signatures.
- Authentication with Public Key Encryption
- Authentication with a Revised Mode of Public Key Encryption
- Authentication with a Pre-Shared Key

More information: http://www.ietf.org/rfc/rfc2409.txt