

Securing IP Networks with Implementation of IPv6

R.M.Agarwal

DDG(SA), TEC

Security Threats in IP Networks

- *Packet sniffing*
- *IP Spoofing*
- *Connection Hijacking*
- *Denial of Service (DoS) Attacks*
- *Man in the Middle (MITM) Attack*

Solutions to these and other types of attacks are not always available.

Security Goals and implementation methods

Security Goals

- Authentication
- Integrity
- Confidentiality

Implementation Methods in IP Networks

- Encryption
- Secure hashes
- Digital Signatures

Implementation Levels

- Possible in every layer of TCP/IP Stack, including IP layer (IPSec)
- Transport Layer through TLS

What is IPsec?

IPsec defines the method that allows a node to encrypt and / or authenticate packets and encapsulate the secured packets (which may now be literally indecipherable, due to encryption) into new packets and transport them across a network.

The goal of IPsec is to provide security for all versions of IP (i.e. both IPv4 and IPv6). But it is

Optional in IPv4 and
Mandatory in IPv6

IP Security Issues

(Features are enabled by IPsec)

- 1. Encryption**
- 2. Authentication**
- 3. Access Control**
- 4. Integrity verification (connectionless integrity)**
- 5. Protection against “replay” attacks**
- 6. Limitation of “traffic analysis” attacks**
- 7. End-to-end security**
- 8. Secure tunneling**

IPsec Protocol Implementation

An IPsec implementation operates in a host, as a security gateway (SG), or as an independent device, affording protection to IP traffic. IPsec security services are offered at the IP layer through selection of appropriate security protocols, cryptographic algorithms, and cryptographic keys.

Encryption and Authentication Algorithms

- **Symmetric encryption**
- **Public key encryption**
- **Key Exchange**
- **Secure hashes**
- **Digital signature**

ESP and AH Headers

All the security functions in IPsec are possible through the use of ESP (Encapsulating Security Payload) header and AH (Authentication Header).

ESP provides mechanisms for applying any kind of cryptographic algorithm to an IP packet including encryption, digital signature, and / or secure hashes.

AH provides mechanisms for applying authentication algorithms to an IP packet.

AH

Provide integrity and authentication without confidentiality to IP datagrams

Implementation Scenarios

- Security between 2 or more hosts implementing AH,
- Security between 2 or more gateways implementing AH,
- Security between a host and gateway implementing AH and a set of host or gateways.

Protocol Structure - IPsec AH: IP Authentication Header

8	16	32bit
Next Header	Payload Length	Reserved
Security parameters index (SPI)		
Sequence Number Field		
Authentication data (variable)		

ESP

Provide Integrity, Authentication and Confidentiality to IP datagrams

Implementation Scenarios

- Security between 2 or more hosts implementing ESP
- Security between 2 or more gateways implementing ESP
- Security between a host or gateway implementing ESP and a set of hosts and /or gateways

Protocol Structure - ESP: Encapsulating Security Payload

16

24

32bit

Security Parameter Index (SPI)

Sequence Number

Payload data (variable length)

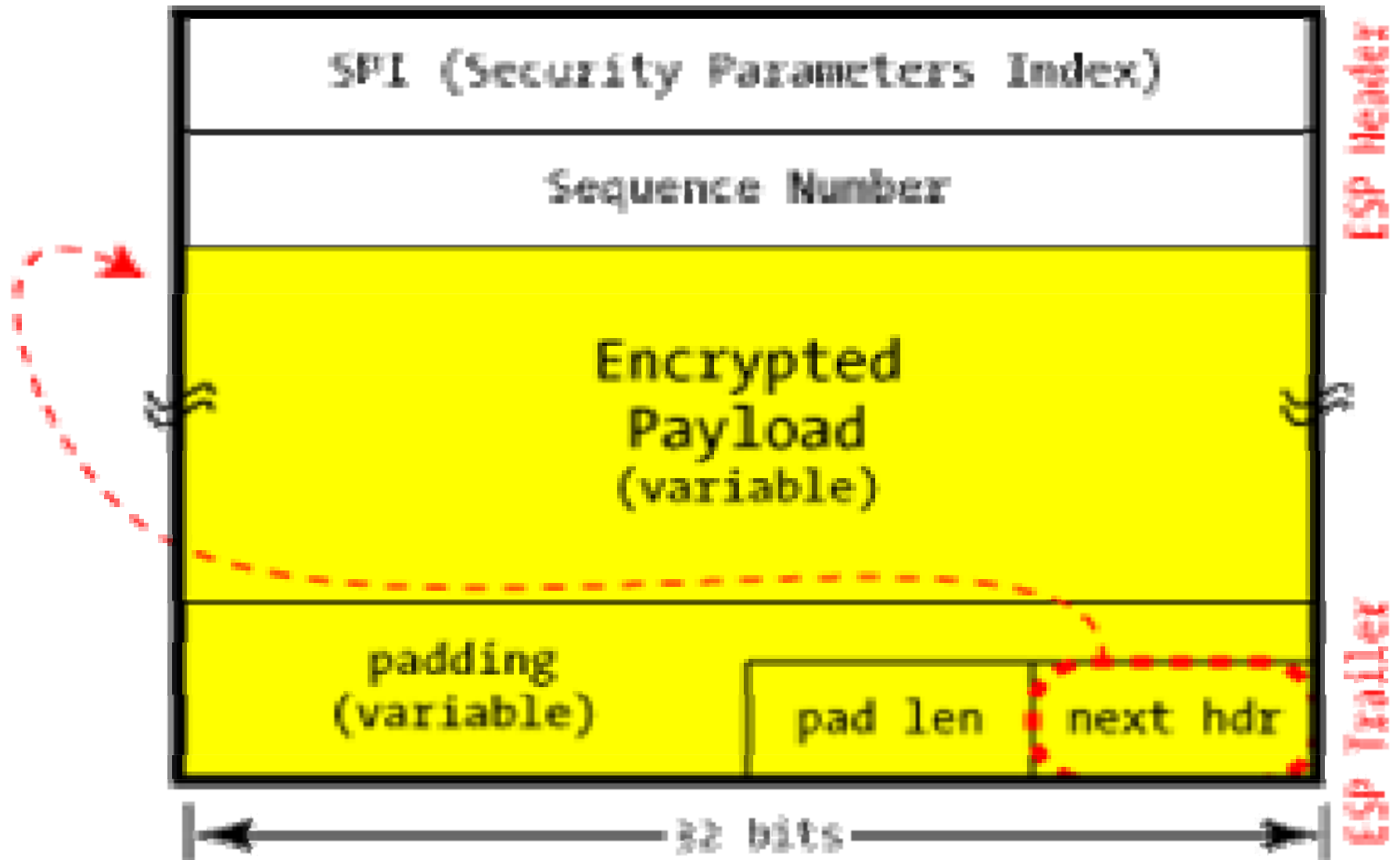
Padding (0-255 bytes)

Pad Length

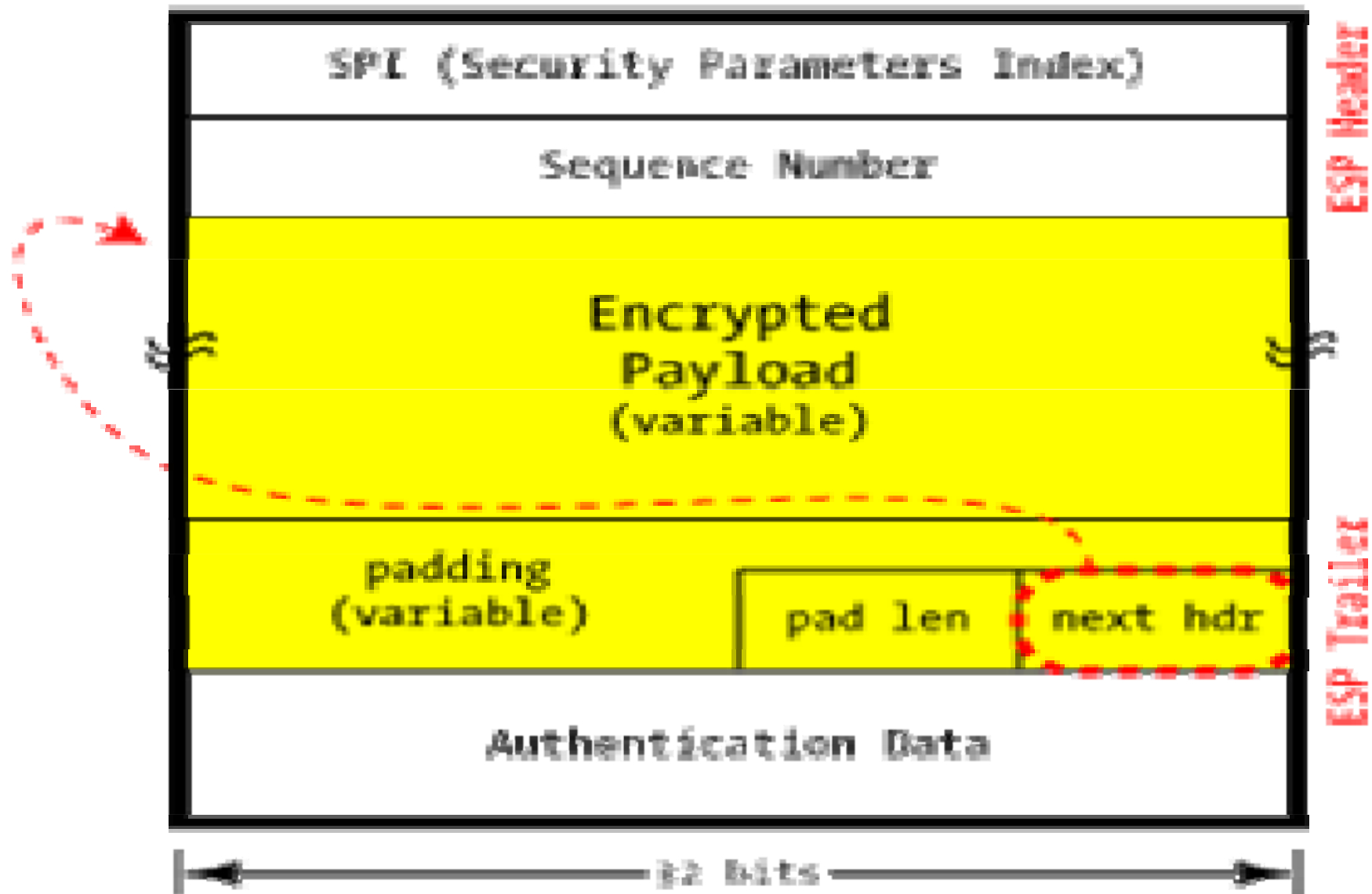
Next Header

Authentication Data (variable)

ESP w/o Authentication



ESP with Authentication



IPSec Implementation Modes

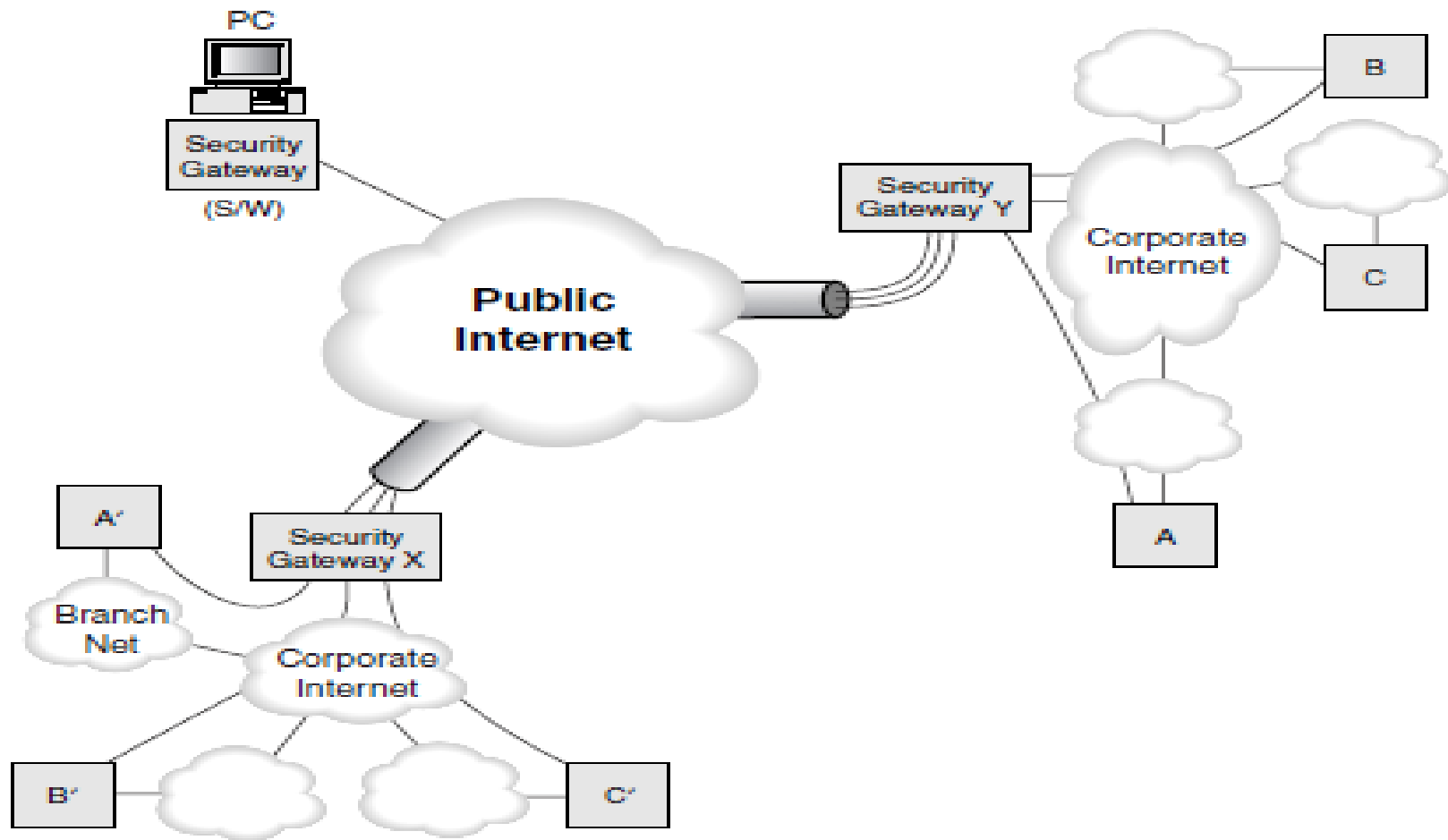
Tunnel Mode

In tunnel mode, AH and ESP are applied to tunneled IP packets.

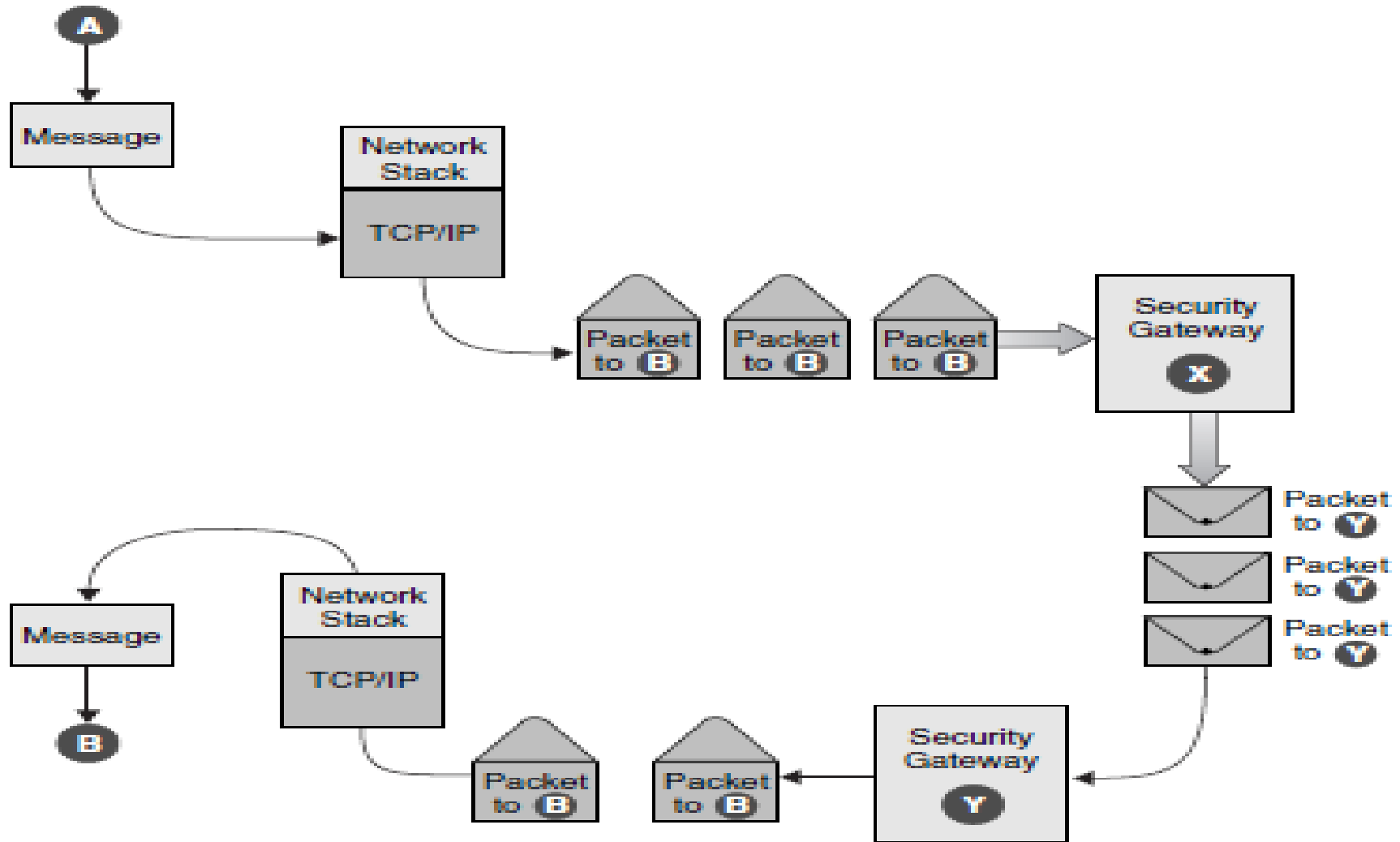
Transport Mode

In transport mode, AH and ESP provide protection primarily for next layer protocols

Security Tunneling through a Hostile Network



Security Tunneling through a Hostile Network



A pair of hosts 'A' and 'B' communicating in the Transport Mode



Security Policy

- A *security policy* is a rule that is programmed into the IPsec implementation that tells it how to process different packets received by the device
- Security policies for a device are stored in the device's *Security Policy Database (SPD)*
- Outbound packets are checked against the SPD to determine the kind of IPsec processing to apply

Security Associations (SA)

- Security Association (SA) is fundamental to IPsec implementation.
- SA is much more specific than a Security Policy
- SA is a “**simplex connection**”
- Each SA will provide security using either AH or ESP but not both
- If both AH and ESP are used by a traffic stream, there will be two SA for that traffic stream

Components of SA

- Security Parameter Index (SPI)
- IP destination Address
- Security Protocol (AH or ESP) identifier

Using Security Associations (Key Exchange Protocols)

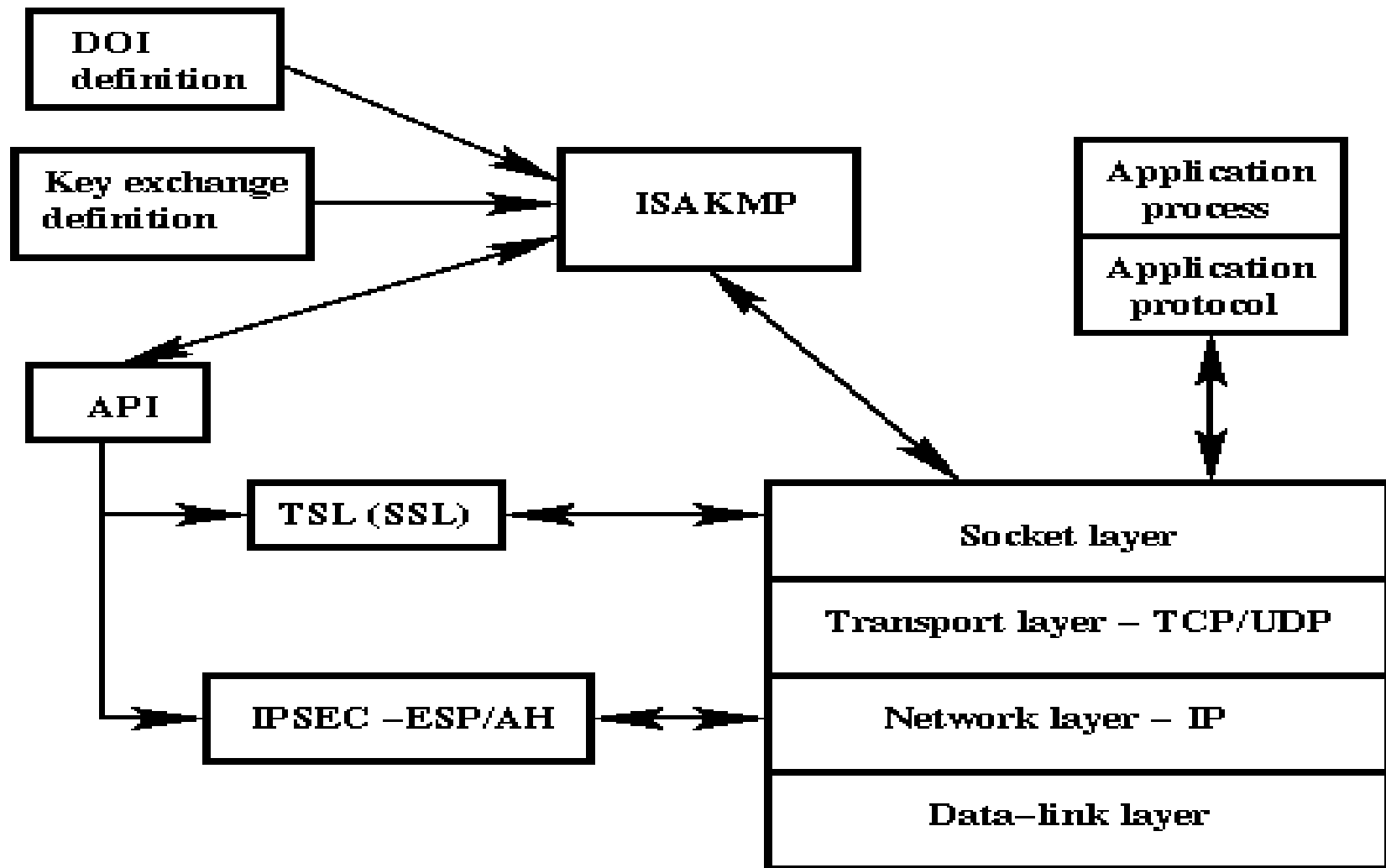
Internet Security Association and Key Management protocol (ISAKMP)

- ISAKMP provides a generalized protocol for establishing SAs and managing the cryptographic keys within an internet environment

Internet Key Exchange (IKE) protocol

- Working within the framework of ISAKMP, it defines the mechanism for hosts to perform negotiation of SAs and authenticated keying material.

Key Management using ISAKMP



Implementing and Deploying IPsec

- **Integrated implementation** - IPsec is integrated into the native IP implementation
- **Bump in the Stack (BITS)** - IPsec is implemented “beneath” the IP stack and “above” the local network drivers
- **Bump in the wire (BITW)** - implements IPsec in a hardware cryptographic processor

Conclusion

- Network security is a critical issue with modern networks working in real world situations.
- Hackers are always on the prowl to attack the networks to derive all possible benefits.
- IPsec exists for IPv4 but it was made **optional** . Therefore, end-to-end security is not guaranteed
- IPsec is made **mandatory** in IPv6. Therefore, it guarantees end-to-end security

Selected References

- Cisco Press, *Deploying IPv6 networks*
- http://72.34.43.90/IPV6/usipv6_reston_2004/wed/Trhulj.pdf (accessed on 12/02/2010)
- <http://www.6journal.org/archive/00000182/01/ipv603.pdf> (accessed on 12/02/2010)
- http://www.cisco.com/web/SI/expo2009/assets/docs/IPv6_Security_groznje_in_mehanizmi_zascite_Eric_Vyncke.pdf (accessed on 12/02/2010)
- <http://www.is-journal.org/V02I02/2ISJLP231-Rowe%20and%20Gallaher.pdf> (accessed on 12/02/2010)
- http://www.v6summit.com/Conference/Presentations/SECURITY_COLLIGNON.pdf (accessed on 12/02/2010)
- Joseph Davies, *Understanding IPv6*, Microsoft Press
- Pete Loshin, *IPv6: Theory, Protocols and Practice*, Elsevier Publications, 2nd edition
- RFC 1825
- RFC 2401
- RFC 4301
- Silvia Hagen, *IPv6 essentials*, O'Reilly Publications