Internet Security

S K Madhukar
ADG (NT)

Internet Security

IPv4 was not designed with security in mind.

Packet Sniffing: Due to network topology, IP packets sent from a source to a specific destination can also be read by other nodes, which can then get hold of the payload (for example, passwords or other private information).

IP Spoofing: IP addresses can be very easily spoofed both to attack those services whose authentication is based on the sender's address (as the rlogin service or several WWW servers).

Connection Hijacking: Whole IP packets can be forged to appear as legal packets coming from one of the two communicating partners, to insert wrong data in an existing channel.

Internet Security

Shortage of IP Address : Lack of visibility and transparency

Data is open to all : No Confidentiality

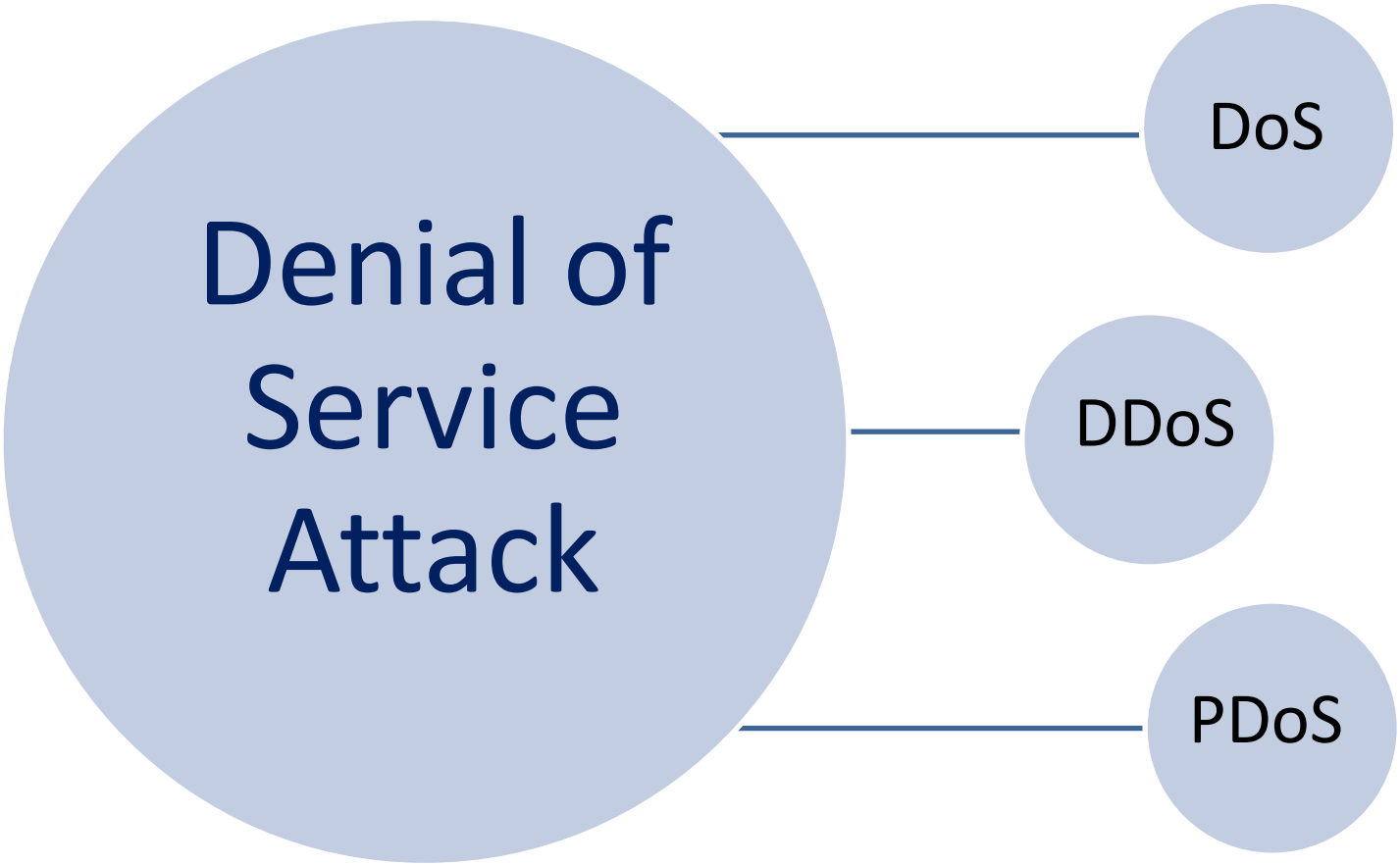
Not Designed for any inbuilt Security Feature

Inherent absence of any tool to ensure integrity of the data

Small Subnet address space helps quick Scanning of Port : Vulnerable to attacks

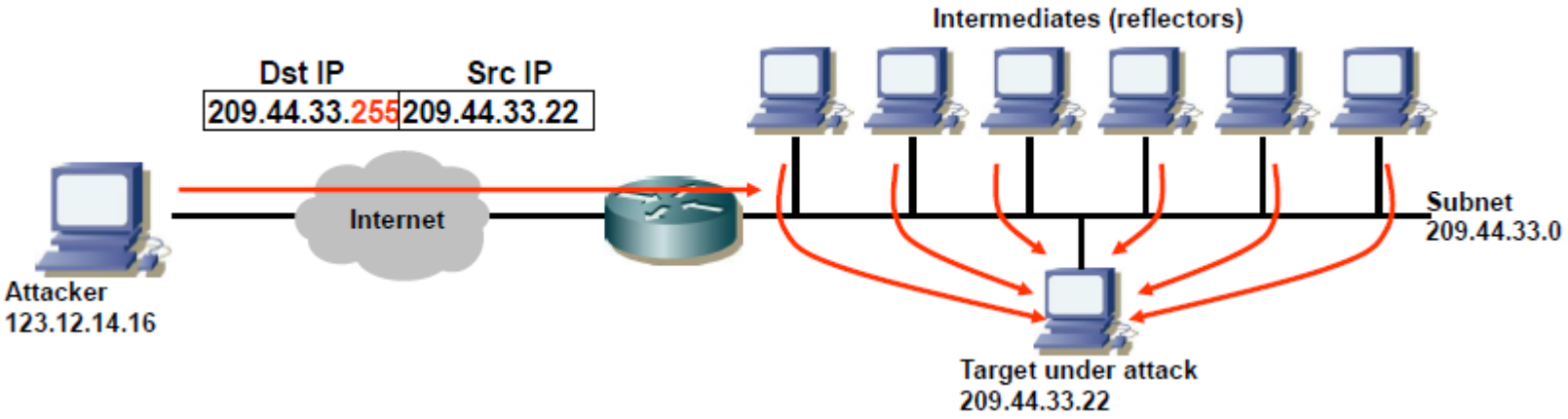
No provision of Load Balancing helps to achieve Denial of Service (DoS) attack

Internet Security



Internet Security

- Flood network with pings (ICMP echo replies) with
- IP destination address = directed network broadcast and
- IP source address = target IP address (spoofed IP address).
- Consumption of target network bandwidth and target processing power.



Internet Security

Procedure:

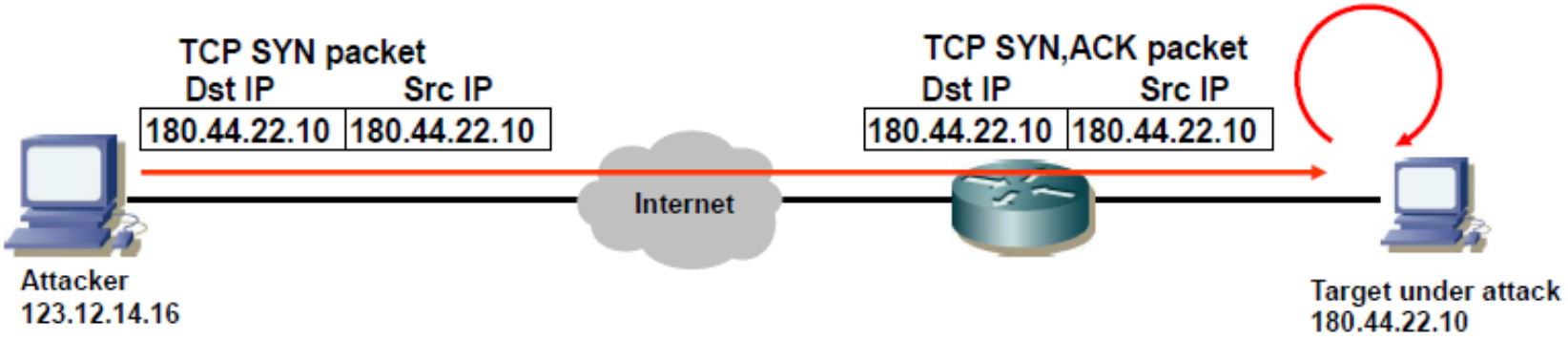
Send a TCP SYN packet with spoofed IP addresses where destination and source IP address are set to the target's IP address.

Effect:

Target sends ACK to itself creating an ACK war.

Counter measures:

OS patches.



Internet Security

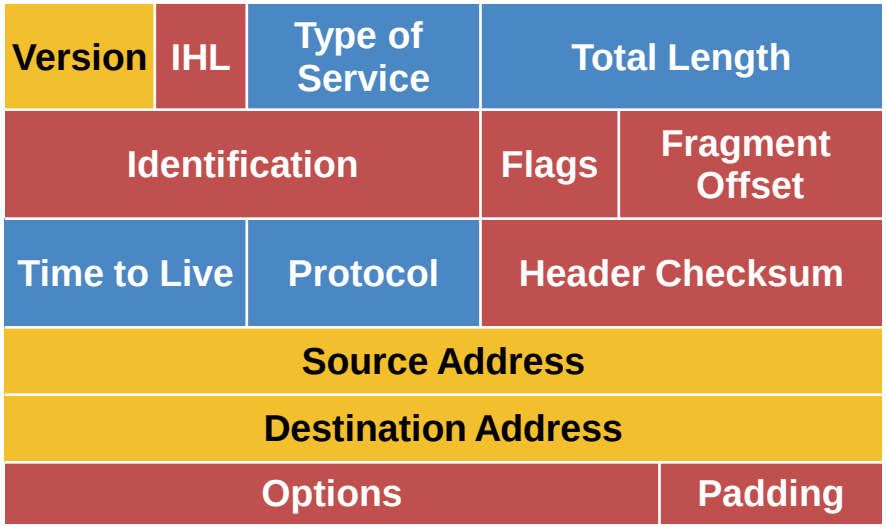
- Architectural vulnerability of IPv4 is the broadcast flooding attack or Smurf attack

- There is no broadcast in IPv6 & first hop Security can be enforced.

Internet Security

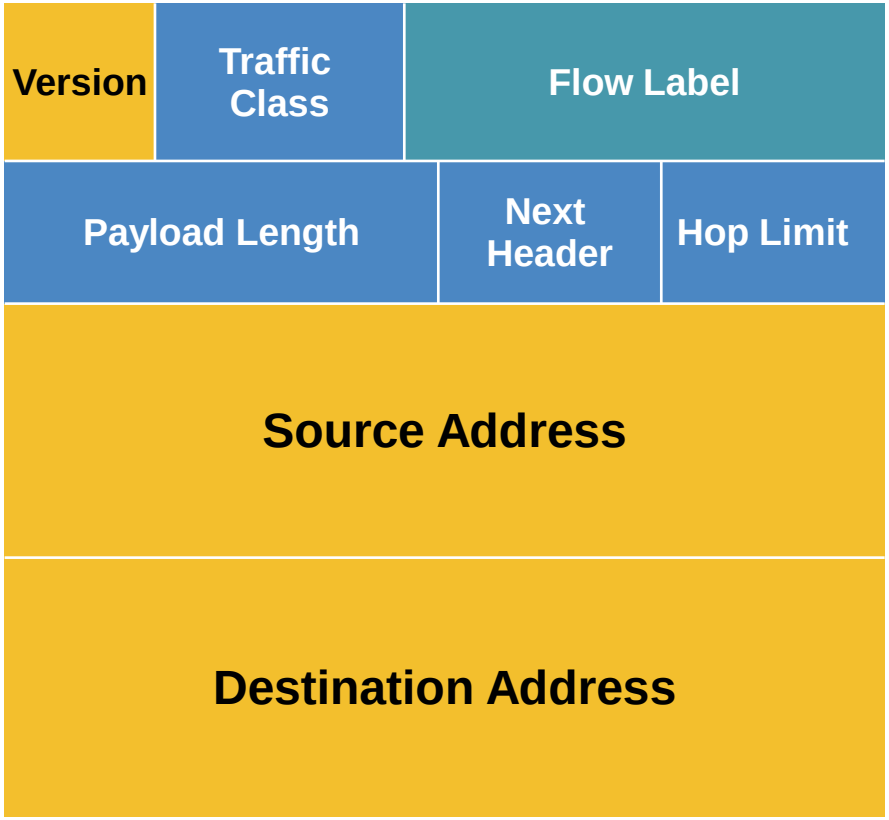
IPv4: 20 Bytes + Options

IPv4 Header



IPv6: 40 Bytes + Extension Header

IPv6 Header



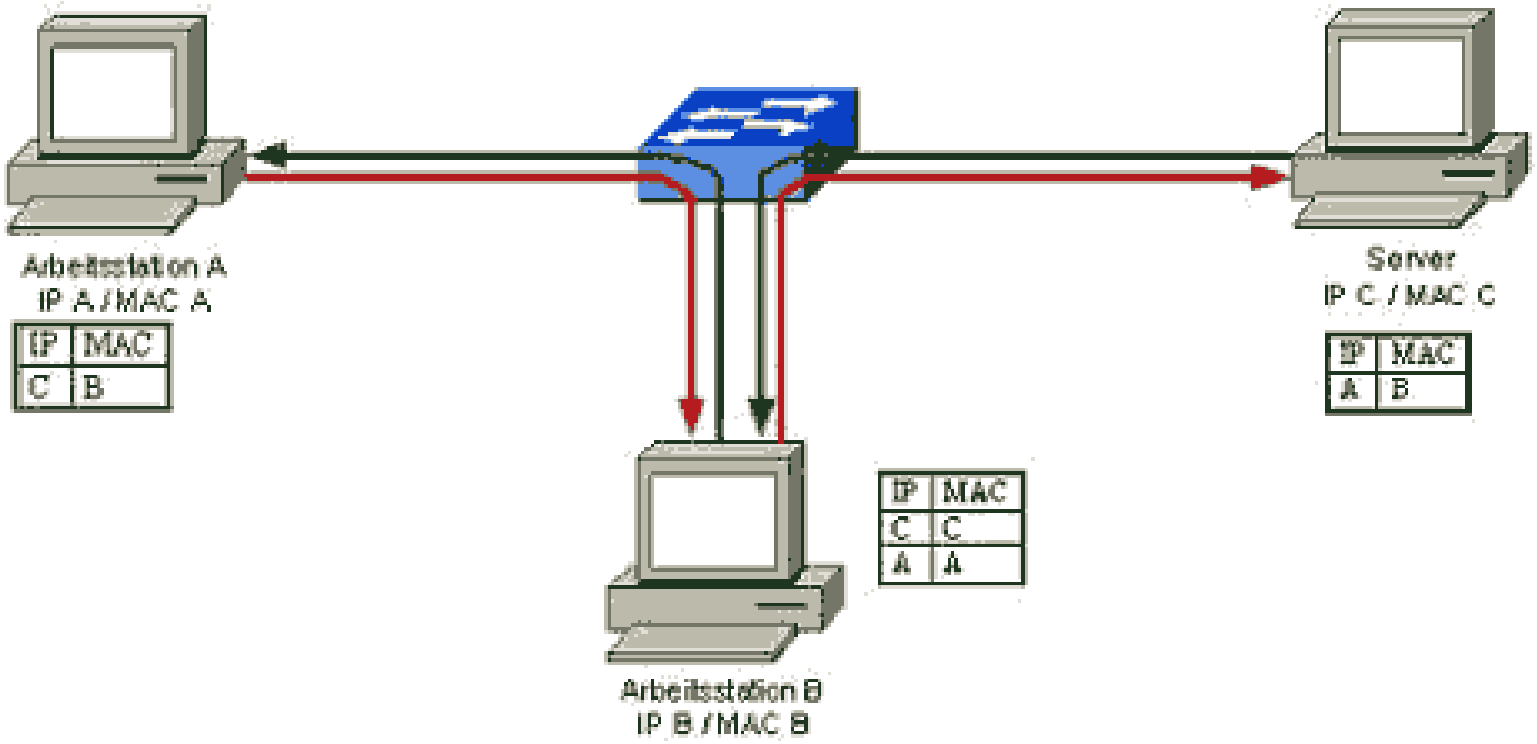
Internet Security

Malicious Code Distribution over network

- Small Address Space of Ipv4 can facilitate Malicious code Implantation/Distribution
- Huge Address Space of IPv6 make this difficult

Internet Security

ARP Poisoning and ICMP redirect



Internet Security

Man in the Middle Attack

- IPv4's lack of proper authentication mechanism may facilitate this in combination of ARP Poisoning and ICMP redirects.

- In IPv6, ARP is not used and proper authentication is essential.

Internet Security

Fragmentation Attack

- Fragmentation and Reassembly in IPv4 may facilitate such attacks like ‘Ping of Death’ etc

- In IPv6, fragmentation is not allowed. Packet size is fixed for ‘end to end’.

Internet Security

Replay Attack

- No mechanism is available in IPv4 to check such attacks

- In IPv6, Sliding Window mechanism is followed.

Internet Security

- Viruses
- Worms
- Trojan Horses
- Spyware
- Botnet

Internet Security Issues

Viruses and Worms :

Viruses and Email, IM worms: IPv6 brings in identification.

Other worms:

- **IPv4: reliance on network scanning**
- **IPv6: not so easy**

IPv4 best practices around worm detection and mitigation remain valid.

IPS systems and Anti-viruses will not change.

Internet Security Issues

IPv4 was not designed with security in mind.

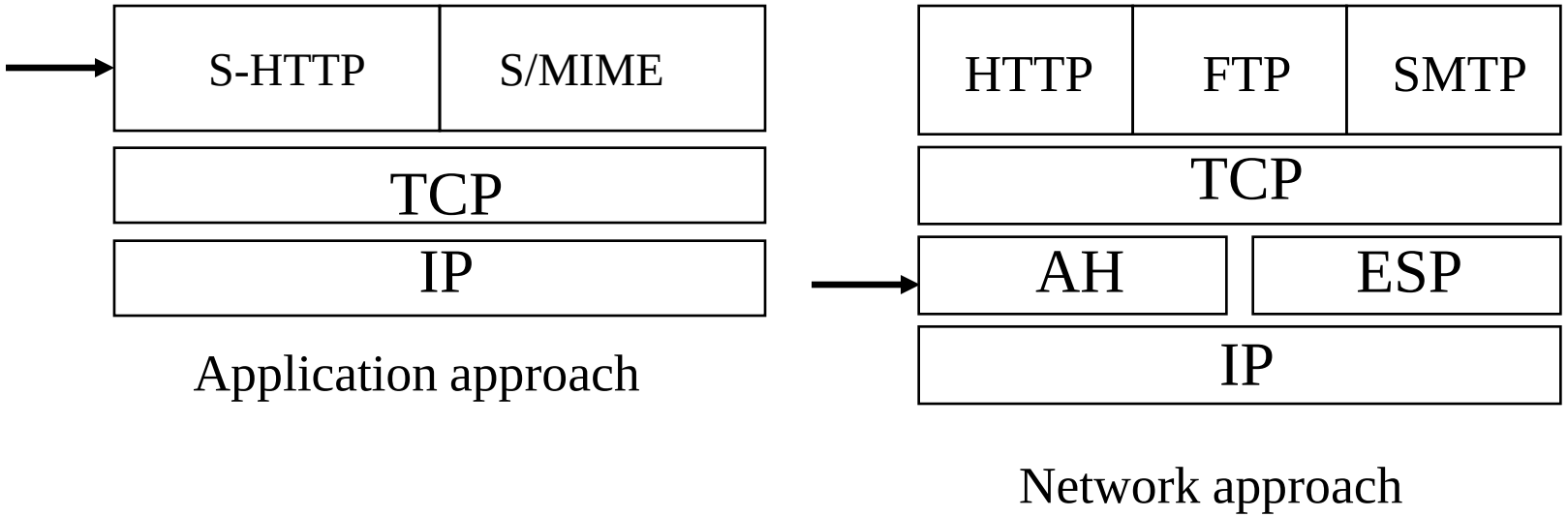
In IPv4, Security is implemented in:

In Applications – HTTPS, IMAPS, SSH etc.

IPsec tunnels

Internet Security Issues

IPsec Services



Internet Security Issues

IPv6 IPSec:

Applies to both IPv4 and IPv6:

- **Mandatory for IPv6**
- **Optional for IPv4**

Applicable to use over LANs, across public & private WANs, & for the Internet

IPSec is a security framework

- **Provides suit of security protocols**
- **Secures a pair of communicating entities**
- **Two different modes: Transport mode (host-to-host) and Tunnel Mode (Gateway-to-Gateway or Gateway-to-host)**

Internet Security Issues

Services Provided by IPsec

Authentication – ensure the identity of an entity (integrity) and replay protection

Confidentiality – protection of data from unauthorized disclosure

Key Management – generation, exchange, storage, safeguarding, etc. of keys in a public key cryptosystem

Internet Security Issues

IPsec Services

Authentication: AH (Authentication Header - RFC 4302)

Confidentiality: ESP (Encapsulating Security Payload - RFC 4303)

Key management: IKEv2 (Internet Key Exchange - RFC4306)

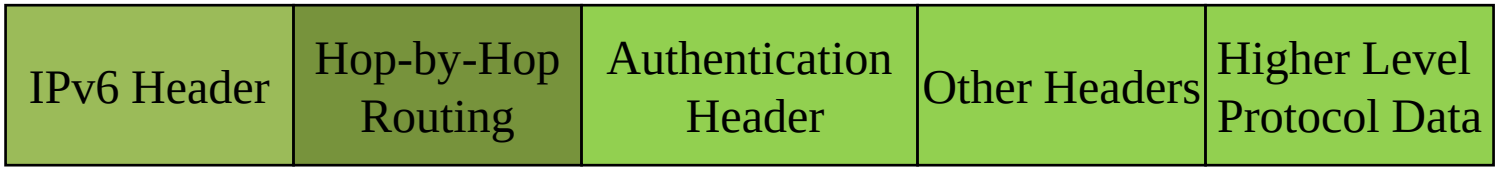
When two computers (peers) want to communicate using IPSec, they mutually authenticate with each other first and then negotiate how to encrypt and digitally sign traffic they exchange. These IPSec communication sessions are called security associations (SAs).

Internet Security Issues

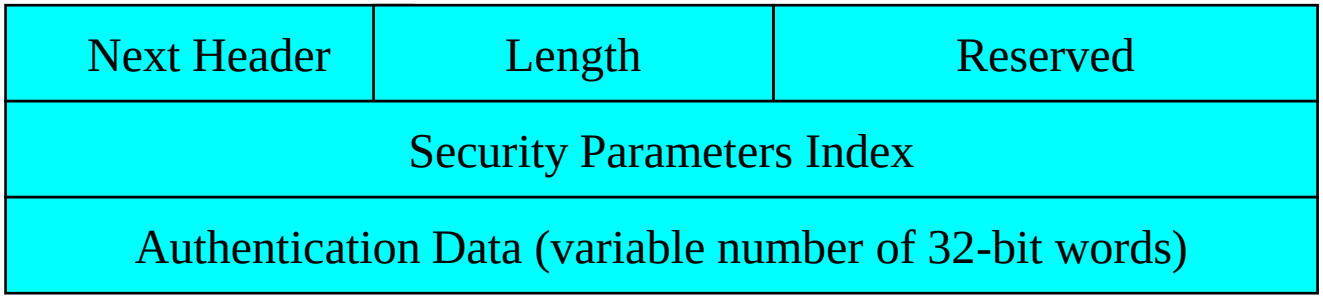
IPv6 IPsec Protocol

IPsec AH

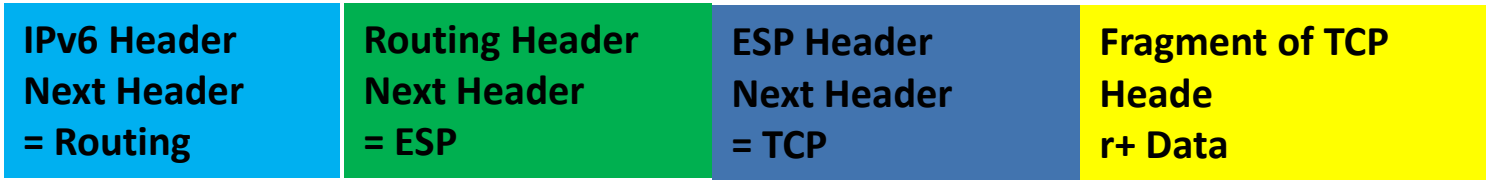
IPv6 AH Packet Format



IPv6 AH Header Format



Internet Security



- IPSec is optional in IPv4
- Requirement in IPv6

Questions .. ?


THANK YOU

Internet Security Issues

- IPv4 - NAT breaks end-to-end network security
- IPv6 - Huge address range – No need of NAT

Reconnaissance In IPv6:

- Default subnets in IPv6 have 2^{64} addresses
- Scan with 10 Mpps will take more than 50 000 years
- Ping sweeps on IPv6 networks are not possible

Internet Security

Port Scanning and other Reconnaissance Attack

- 2^8 hosts X 1sec => 4.267 Minutes
- 2^{64} hosts X 1sec => 5.8 Th Th Yrs

Scanning is almost impossible in case of IPv6

Additional Feature Available in IPv6

IPSec

- Authentication Header (AH)
- Encapsulation Security Protocol (ESP0
- Internet Key Exchange (IKE)

IPSec

Authentication Header (AH)

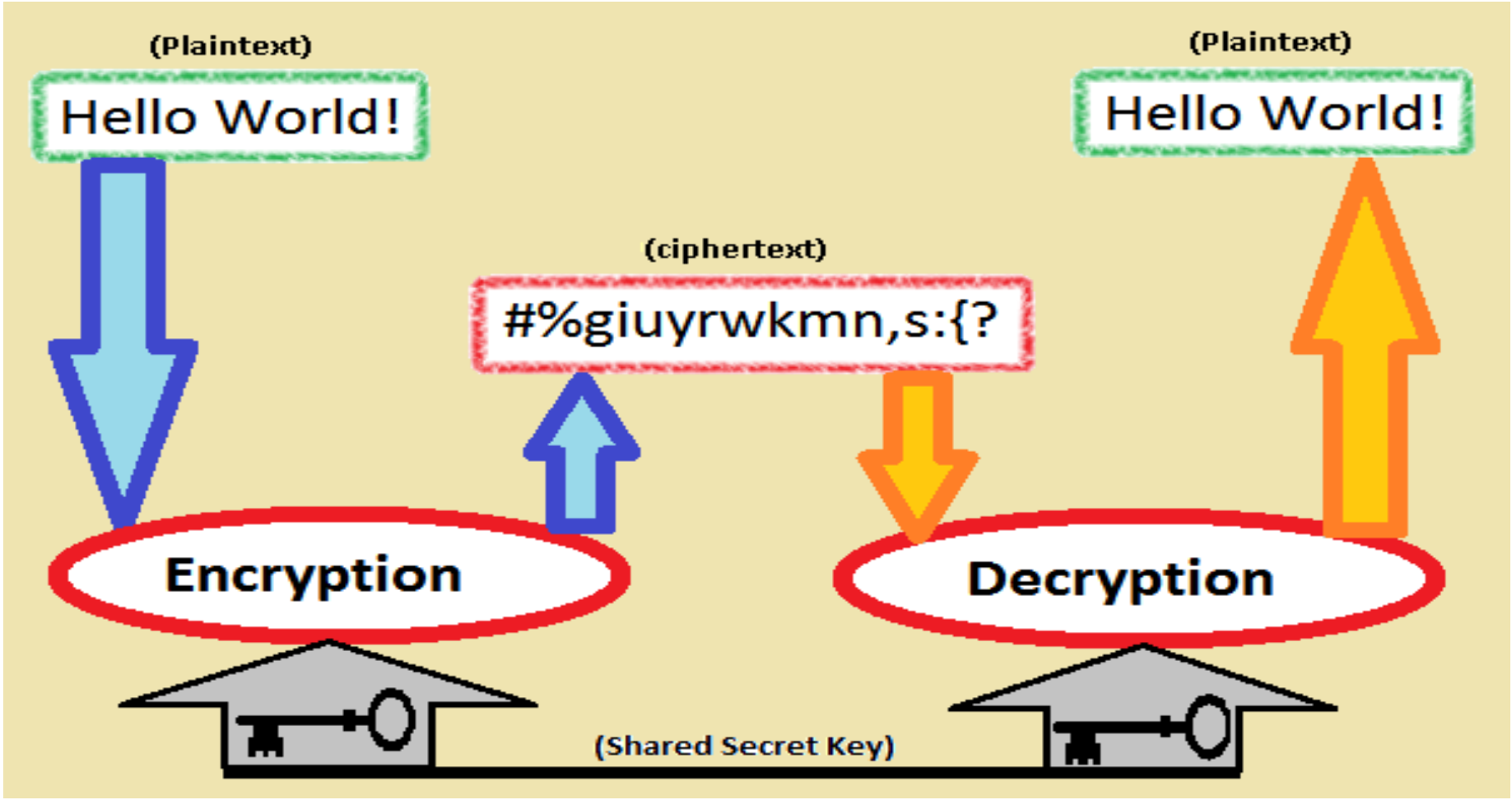
- Source Authentication
- Data Integraty

IPSec

Encapsulation Security Protocol (ESP)

- Authentication
- Data Integrity
- Confidentiality

IPv6 Header Next Header = Routing	Routing Header Next Header = ESP	ESP Header Next Header = TCP	Fragment of TCP Heade r+ Data



IPsec

Internet Key Exchange (IKE)

- Initial Functionality and Negotiating between End to End Node
- Keep track of information so that the security is guaranteed