Bkav

Bkav 2013

Hãy làm việc **hết mình, những điều tốt đẹp** sẽ đến với bạn !

Những lợi thế và thách thức của IPv6 Security

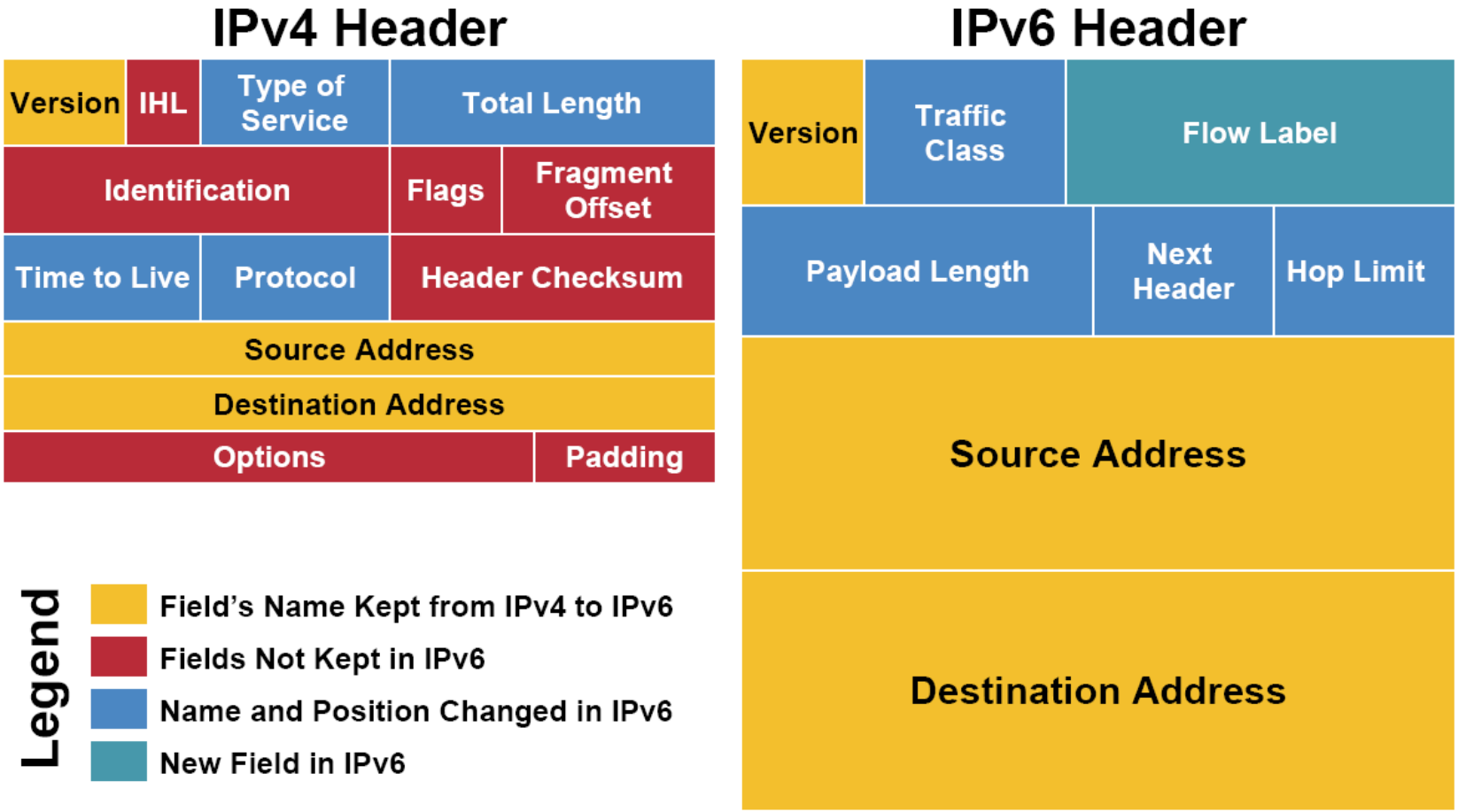
Nguyễn Minh Đức

Khác biệt về security giữa IPv6 và IPv4

IPv6 bao gồm các RFCs

- RFC 24602: IPv6 Protocol
- RFC 48613: IPv6 Neighbour Discovery
- RFC 48624: IPv6 Stateless Address Auto-Configuration
- RFC 44435: Internet Control Message
- Protocol for IPv6 (ICMPv6)
- RFC 42916: IPv6 Addressing Architecture
- RFC 43017: Security Architecture for IP or IPsec

IPv4 và IPv6 Header



Source: TCPIP6

Các vấn đề về security của IPv4

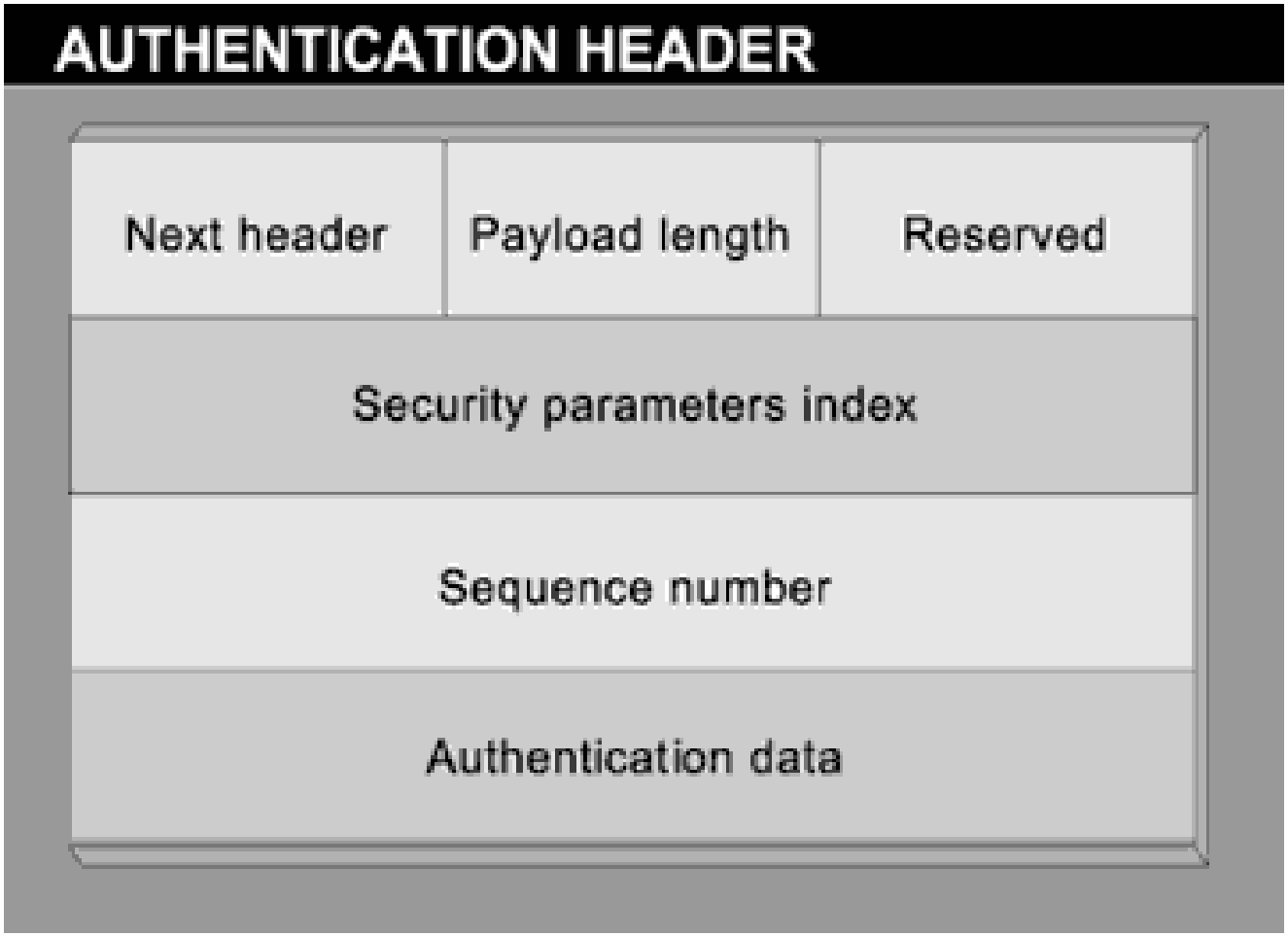
- Denial of service attacks (DOS)
- Phát tán mã độc
- Tấn công dạng MITM (Man-in-the-middle)

IPv6 vs IPv4 Security

1. Không gian địa chỉ IP lớn hơn
2. IP Security (IPSec)
3. Neighbour Discovery (ND) Protocol thay thế cho ARP

Lợi thế về security của IPv6

IPSec: Authentication Header



Source: GMU

IPSec: Authentication Header

IPv6----Before applying AH

Original IPv6 Header	Extension Header if present	TCP	Data

IPv6----After applying AH (transport mode)

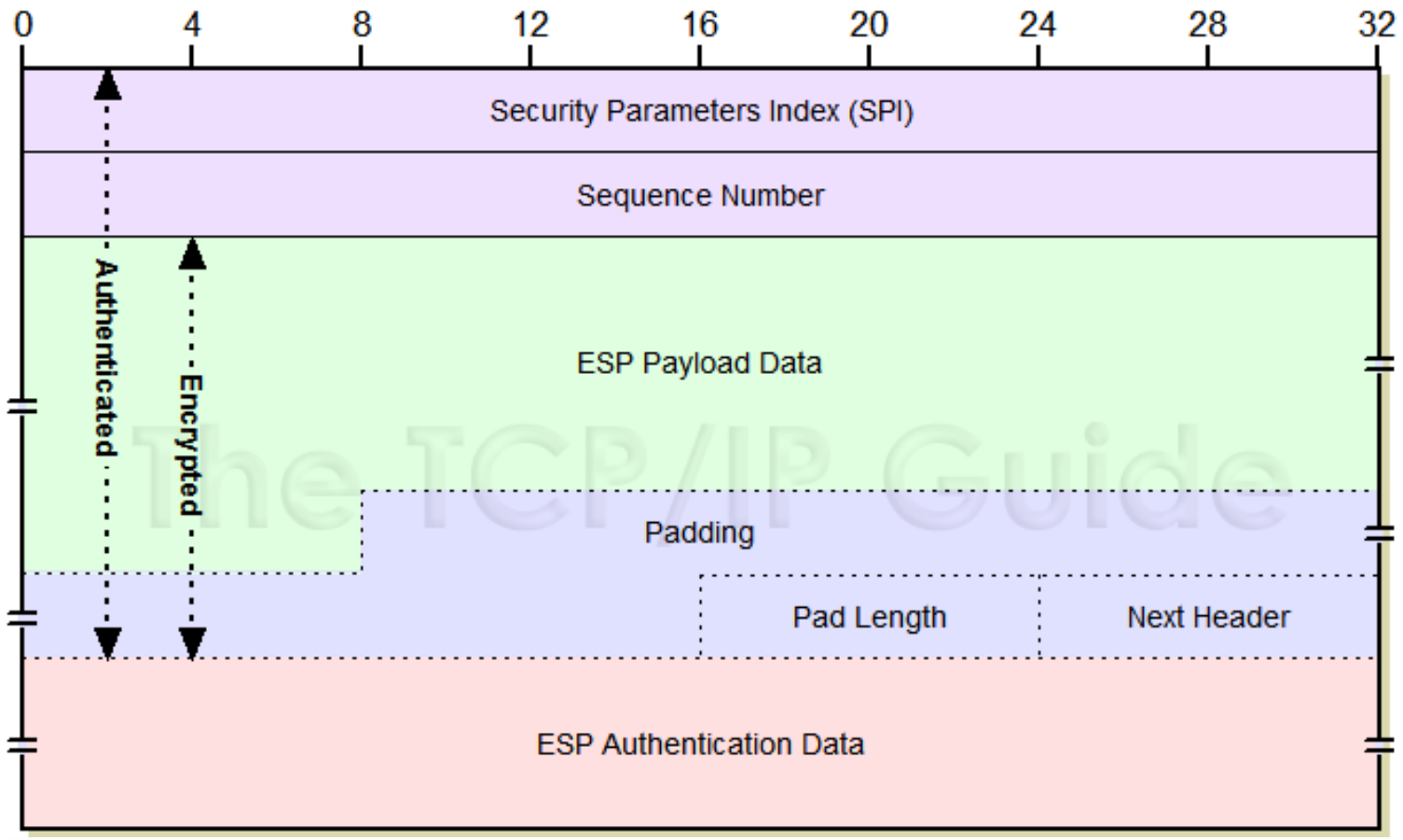
Original IPv6 Header	Extension Header if present *	AH	Dest. *	TCP	Data

*: If destination extension header presents, it could be before AH, after AH or both

IPv6----After applying AH (tunnel mode)

New IPv6 Header	New Extension Headers if present	AH	Orig IPv6 Header	Extension Headers if present	TCP	Data

IPSec: Encapsulating Security Payload Header



Source: The TCP/IP Guide

Neighbour Discovery (ND) Protocol

IPv4 "Neighbor Related" Protocol Stack

Application	HTTP FTP, Telnet, etc.	RIP RADIUS Traceroute DNS, etc.	PING	Router Discovery Path MTU Discovery Redirect				
Transport	TCP	UDP			RTP, SCTP, etc.			
Network	IP		ICMPv4			ARP	RARP	IPCP
Data Link	Ethernet/802.3 Token Ring (802.5) SNAP/802.2 X.25 FDDI ISDN Frame Relay SMDS ATM Wireless Fibre Channel DDS/DS0/T-carrier/Ecarrier, SONET/SDH DWDM PPP HDLC SLIP/CSLIP xDSL Cable Modem (DOCSIS)							

IPv6 Neighbor Discovery Protocol Stack

Application	HTTP FTP, Telnet, etc.	RIP RADIUS Traceroute DNS, etc.	PING	Neighbor Discovery/ Inverse ND				
Transport	TCP	UDP			RTP, SCTP, etc.			
Network	IPv6		ICMPv6					
Data Link	Ethernet/802.3 Token Ring (802.5) SNAP/802.2 X.25 FDDI ISDN Frame Relay SMDS ATM Wireless Fibre Channel DDS/DS0/T-carrier/Ecarrier, SONET/SDH DWDM PPP HDLC SLIP/CSLIP xDSL Cable Modem (DOCSIS)							

Source: Realccielab

Một số thách thức đối với IPv6

Một số thách thức đối với IPv6

- Tấn công ở tầng ứng dụng
  - Web, Buffer Over Flow, mã độc...
  - Lừa đảo trực tuyến
  - Password Bruteforce
  - DoS và DDoS
- Truy tìm nguồn tấn công

Kết luận

- IPv6 là một sự cải tiến đáng kể đối với IPv4
- IPv6 được thiết kế với định hướng đảm bảo an toàn và có nhiều ưu điểm tốt hơn IPv4 về bảo mật
- Vẫn có thể có một số vấn đề về security mà các tầng khác cần giải quyết để hỗ trợ cùng IPv6

Xin cảm ơn