中山大學
SUN YAT-SEN UNIVERSITY

Module II. Internet Security

Chapter 4
Introduction to Internet Security

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **4.1 Network Security Architectures**
  - Five Layers of Network Security Architectures
  - Information Security Models
  - OSI/ISO 7498-2
  - ISO Security Services
  - ISO Security Mechanisms
- **4.2 IPSec**
  - Introduction
  - Some Basic Concepts about IPSec
  - ESP protocol √
  - Gateway and Road Warrior Mode
  - Key Management of IPSec

Outline

- **4.3 SSL/TLS**
  - Introduction
  - How TLS Works
  - Decryption of TLS Packet
- **4.4 VPN**
  - Introduction to IPsec VPN
  - OpenVPN

4.2 IPSec

4.2.1. Introduction

- **What is IPsec**
  - IPsec, Internet Protocol Security, is officially specified by IETF.
    - ✧ IETF, the Internet Engineering Task Force
    - ✧ Request for Comment: RFC-1825 to RFC-1827
  - IPsec is a protocol suite.
    - ✧ IPsec is a protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

4.2 IPSec

4.2.1. Introduction

- **What is IPsec**
  - IPsec is an end-to-end security scheme.
    - ✧ IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).
  - IPsec protects any application traffic across an IP network.
    - ✧ Applications do not need to be specifically designed to use IPsec.
    - ✧ Some other Internet security systems in widespread use operate in the upper layers of the TCP/IP model.
      - ◌ such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH)
      - ◌ The use of TLS/SSL must be designed into an application to protect the application protocols.

4.2 IPSec

4.2.1. Introduction

- **What is IPsec**
  - IPsec is a successor of the ISO standard Network Layer Security Protocol (NLSP).
    - ✧ NLSP was based on the SP3 protocol that was published by NIST, but designed by the Secure Data Network System project of NSA.

4.2 IPSec

4.2.1. Introduction

- **What is IPsec**
  - IP 协议的安全性
    - ✧ 传统的 IP 协议诞生于军用计划，设计之初未考虑太多安全问题，存在很多安全隐患。
    - ✧ 比如数据明文传输，同在一个集线器的通信可以被互相监听，如果获得交换机权限，所有流经交换机的通信也可以被监听。攻击者即便没有交换机权限，也可以通过中间人攻击窃取用户的通信。
  - IPsec 提供了网络层加密方案
    - ✧ 对 IP 协议进行安全加强的迫切需要催生了 IPsec。IPsec 在网络层将 IP 分组的内容先加密再传输，即便中途被截获，由于缺乏解密数据包所必要的密钥，攻击者也无法获取里面的内容。

4.2 IPSec

4.2.1. Introduction

- **What is IPsec**
  - IPsec 提供了网络层加密方案
    - ✧ IPsec 对数据进行加密的方式有两种：传输模式和隧道模式。
      - ◌ 传输模式只是对 IP 协议的数据部分 (payload) 进行了加密
      - ◌ 隧道模式则是对整个 IP 分组进行加密，就好像整个 IP 数据包在一个安全的隧道里传输一样。

4.2 IPSec

4.2.2 How IPsec Protect Us

- **What Do We Need to Protect**
  - Data Confidentiality 数据保密
    - ✧ 用各种加密手法对数据进行加密，保证攻击者无法破解密密文。
  - Data Integrity 数据完整性度量
    - ✧ 保证所收到的数据是完整的，在传输途中没有被恶意增减或篡改。
  - Origin Authentication 来源认证
    - ✧ 需要确认数据发送和接收两方的身份，防止攻击者的伪造 (例如将数据包截获后将发送地址改成自己的地址，从而诱骗受攻击者将回复包发送给攻击者)。

4.2 IPSec

4.2.2 How IPsec Protect Us

- **What Do We Need to Protect**
  - Prevent Replay-Attack 防止回放攻击
    - ✧ 攻击者有时候并不 (或者无法) 窃取信息，而是进行恶意破坏。比如截获交易命令的数据包后，攻击者虽然无法知道里面的具体的内容，但只要他将交易过程的所有数据包重复发送一次就能造成另一次重复的交易，从而使得被攻击者遭受损失。
    - ✧ 对每一个数据包打上一个唯一的标示，以及时鉴别重复包是一种可行的办法。

4.2 IPSec

4.2.2 How IPsec Protect Us

- **How Does IPsec Provide Us**
  - 数据保密
    - ✧ 使用对称加密技术可以保证加解密操作的速度。由于对称密钥需要通过不安全的网络来传输，所以需要一个保护密钥的机制。非对称密码技术正好能起到这样的保护作用。
    - ✧ 保证了对称密钥的安全之后还需要保证公钥的合法性，即需要确定给我们发送证书的一方不是伪装的攻击者。这个时候，就需要寻求一个可以信任的第三方来为通信双方做身份验证，比如 X.509 证书。IPsec 的密钥传输不仅可以使用 X.509 证书，还可以使用预共享密钥 (PSK) 或 RSA 密钥。

4.2 IPSec

4.2.2 How IPsec Protect Us

- **How Does IPsec Provide Us**
  - 数据完整性度量
    - ✧ 对数据做摘要并将摘要结果附在数据上传输，接收者收到数据后以同样的方式对数据做摘要，再将结果与附在数据后面的摘要进行对比，获得数据的完整性。
    - ✧ 需要考虑摘要算法的碰撞性。(HMAC, Hash-based Message Authentication Code)
  - 来源认证
    - ✧ 来源认证同样以信息摘要的方式来解决，此时的信息摘要中包含了发送方的地址信息。(HMAC)
  - 防止回放攻击
    - ✧ 给数据加上时间戳和随机数，以确保能唯一区分每个新的消息。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **AH Protocol & ESP Protocol**
  - AH 认证头协议
    - ✧ AH, Authentication Headers 协议能够在数据的传送过程中对数据进行完整性度量和来源认证，还可以防止回放攻击。
    - ✧ AH 协议和 ESP 协议相比较具备更强的认证能力，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。 AH 的工作原理是在每一个 IP 数据包上添加一个身份验证报头。此报头包含一个带密钥的 Hash 值 (可以将其当作数字签名，只是它不使用证书)，此 Hash 值在整个数据包中计算，因此对数据的任何更改将致使散列值无效—从而提供了完整性保护。
    - ✧ AH 报头位置在 IP 报头和传输层协议报头之间。AH 由 IP 协议号 51标识，该值包含在 AH 报头之前的协议报头 (如 IP 报头) 中。
    - ✧ AH可以单独使用，也可以与 ESP 协议结合使用。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **AH Protocol & ESP Protocol**
  - ESP 封装安全载荷协议
    - ESP, Encapsulating Security Payloads 协议能够在数据的传输过程中对数据进行完整性度量、来源认证以及加密，也可以防止回放攻击。
    - ESP 服务依据建立的 SA，对可选项目有所限制：
      - 完整性检查和认证一起进行
      - 仅当与完整性检查和认证一起时，Replay 保护才是可选的
      - 重播保护只能由接收方选择
    - ESP 的加密服务是可选的，但如果启用加密，则也就同时选择了完整性检查和认证。因为如果仅使用加密，入侵者可能发动密码分析攻击。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **AH Protocol & ESP Protocol**
  - ESP 封装安全载荷协议
    - ✧ 一般情况下 ESP 不对整个原 IP 包加密，只加密其中不包括 IP 头的有效载荷部分 (传输模式)。但在端对端的隧道通信中，ESP 需要对整个 IP 数据包加密 (隧道模式)。
    - ✧ ESP 报头位置在 IP 报头之后，TCP 或 UDP 等传输层协议报头之前。ESP 由 IP 协议号50标识。
    - ✧ ESP 可以单独使用，也可以和 AH 结合使用。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **Tunnel Mode & Transport Mode**
  - Tunnel Mode 隧道模式
    - ✧ 隧道模式下 IPsec 将要发送的原 IP 报文作为数据内容，在这段“数据”前面加上 ESP 或 AH 协议头，再加上新的 IP 头，形成 IPsec 报文进行传输。
    - ✧ 原 IP 报文的传输就像在一个安全的隧道中进行一样。在整个传输过程中，原报文保持原有的完整结构，内容没有被修改。
  - Transport Mode 传输模式
    - ✧ 传输模式下 IPsec 保护的仅仅是原 IP 报文的数据内容部分 (有效载荷)，而不是整个原报文。在这个过程中原报文结构被修改。
    - ✧ 在处理方法上，原 IP 报文被拆解，在其有效载荷前面加上新的 ESP 或 AH 协议头，再装回原来的 IP 地址，形成 IPsec 报文。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - Need a structure to store keys and related things
    - ✧ SA (Security Association)
  - Need a place to store SAs
    - ✧ SAD (Security Association Database)
  - Need a structure to associate packets with SAs
    - ✧ SPI (Security Parameter Index)
  - Need a place to store policies (or rules)
    - ✧ SPD (Security Policy Database)

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - SA
    - ✧ Security Associations 安全关联。SA 是 IPsec 的重要概念，可以理解为被 IPsec 保护的某个连接的唯一标示。SA 是单向的，即在一次安全的通信中，通信的两个方向 (发送和接收) 各需要创建一个 SA。
    - ✧ 一个 SA 所包含的内容是维护一次安全通信所需要的数据参数。通常，一个 SA 可以由目的地址，IPsec 所采用的协议 (AH或ESP) 和 SPI 来唯一确定。
    - ✧ 所有的 SA 都被存放在一个数据库中，称为 SAD。
    - ✧ SA 的建立和维护通过密钥交换协议 IKE 实现。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - SAD
    - ✧ Security Associations Database 安全关联数据库。每一个 SA 在 SAD 中都会有一个与之对应的条目，保存 SA 的信息。
    - ✧ 通常一个 SAD 条目会包含以下内容：
      - ◌ 顺序号计数器 Sequence number counter for outbound communications
        - 在 AH 或 ESP 的头部，占32比特。SA 初次建立时置0，每发送一个数据包加1。
      - ◌ 顺序号溢出计数器 Sequence number overflow counter
        - 用来标志这个 SA 是否应被弃用。如果顺序号已经溢出，当前的 SA 就应该被抛弃，否则会使得重放攻击成为可能。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - SAD
    - ✧ 通常一个 SAD 条目会包含以下内容：
      - ◌ 防止回放窗口 Anti-replay Window
        - 占32比特。与 TCP 窗口的概念类似，引进窗口的原因是为了实现可靠的传输服务。
      - ◌ SA 有效期 Lifetime of the SA
        - 通过字节计数 (byte count) 或时间帧 (time frame) 或两者的结合来记录一个 SA 的使用时间。若两者一起使用的话，以先到期限的那一个为准。当 SA 使用了一段时间后就应该被删除以确保安全。
      - ◌ AH 协议中所使用的算法以及密钥。默认情况下，IPsec 至少要支持 HMAC-MD5 和 HMAC-SHA，算法需要密钥支持。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - SAD
    - ✧ 通常一个 SAD 条目会包含以下内容：
      - ESP 协议用于认证以及完整性度量的算法以及密钥。
      - ESP 协议用于加密数据的算法以及密钥。
      - IPsec 运行的模式：传输模式 (transport mode) 或者是隧道模式 (tunnel mode)。
      - PMTU (Path MTU)，由 SA 的 ICMP 数据获得。MTU 值是传送数据包大小的最大上限，PMTU 是两个通信设备间的 MTU。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - SPI
    - ✧ Security Parameter Index 安全参数索引。用于将收到的 IPsec 数据包与其对应的 SA 进行关联。
  - SPD
    - ✧ Security Policy Database 安全策略数据库。IPsec 的策略就是规则。SPD 的策略告诉系统如何处理收到的数据包，例如将包处理成 IPsec 数据包从而进行保护，或者不保护直接转发，甚至直接丢弃。
  - IKE
    - ✧ Internet Key Exchange 互联网密钥交换协议。默认情况下，IPsec 使用它来自动管理密钥，也可以直接手动管理。

4.2 IPSec

4.2.3 Some Basic Concepts About IPsec

- **How IPsec Organize All Things Together**
  - HMAC & MAC
    - ✧ A keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key.
    - ✧ As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message.
    - ✧ Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly.

4.2 IPSec

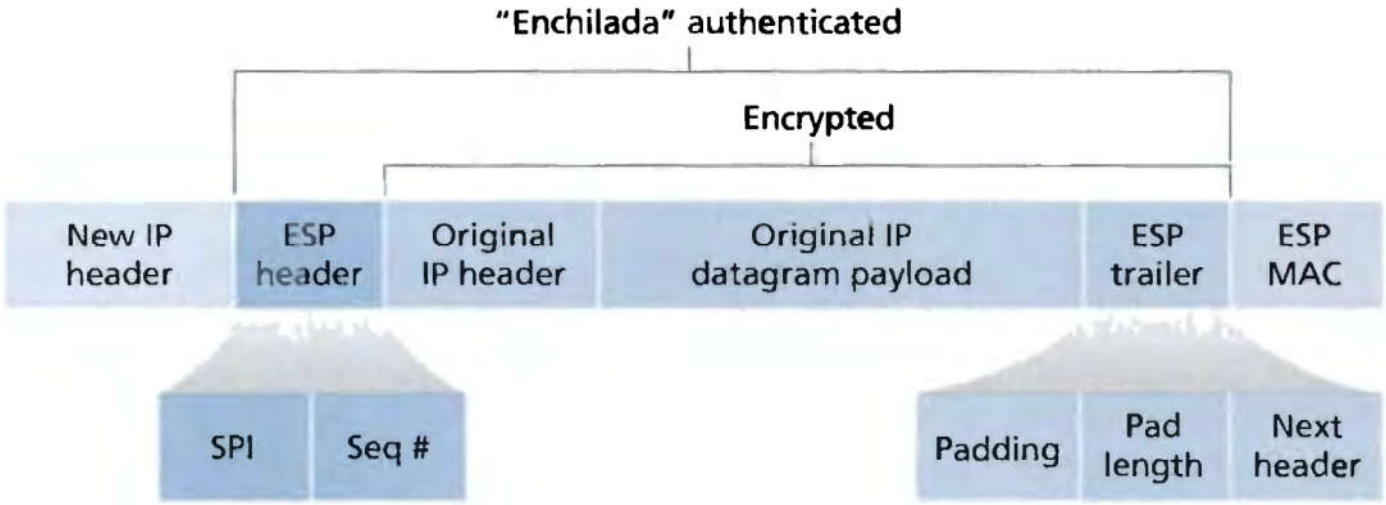
4.2.4 ESP Protocol

- **Tunnel Mode**
  - Encryption of all the IP packet
  - Add new header
  - Just like transmission through a tunnel
- **Transport Mode**
  - Encryption of payloads
  - No encryption of header

4.2 IPSec

4.2.4 ESP Protocol

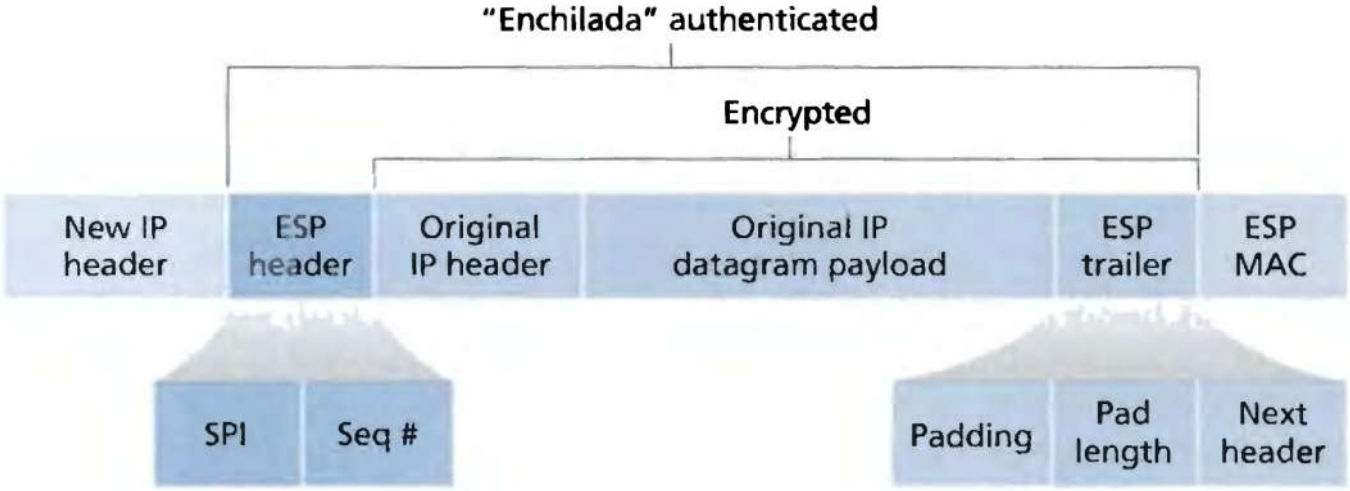
- **IPsec (ESP) Datagram in Tunnel Mode**



4.2 IPSec

4.2.4 ESP Protocol

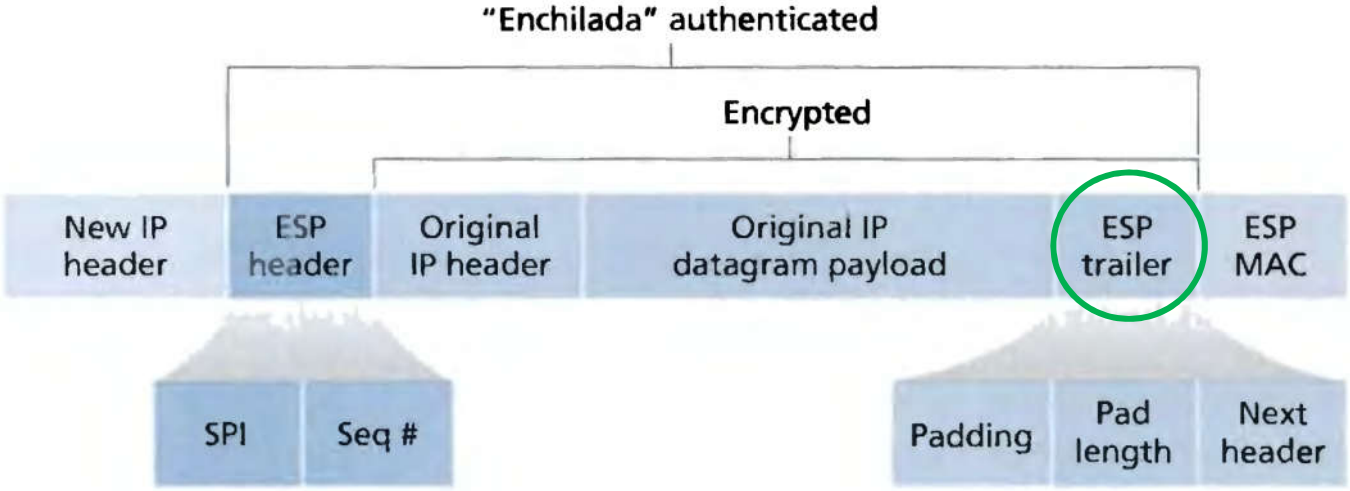
- **IPsec (ESP) Datagram in Tunnel Mode**
  - When a packet is going to be sent
    1. Append an ESP trailer
    2. Encryption
    3. Append an ESP header
    4. Append MAC
    5. Create a New IP Header



4.2 IPSec

4.2.4 ESP Protocol

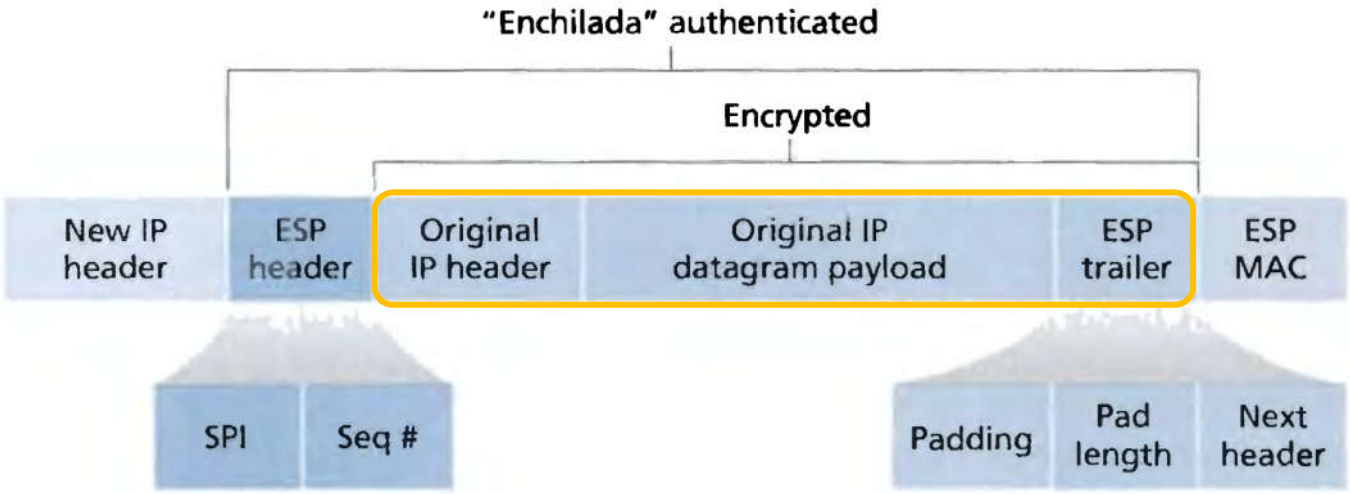
- **IPsec (ESP) Datagram in Tunnel Mode**
  - 装包过程
    1. 在原 IP 报文末尾添加 ESP trailer (尾部/挂载) 信息。
       - ESP trailer 包含三部分。由于所选加密算法可能是块加密，当最后一块长度不足时就需要填充 (padding)，附上填充长度 (Pad length) 方便解包时顺利找出用来填充的那一段数据。Next header 用来标明被封装的原报文的协议类型，例如 4=IP。



4.2 IPSec

4.2.4 ESP Protocol

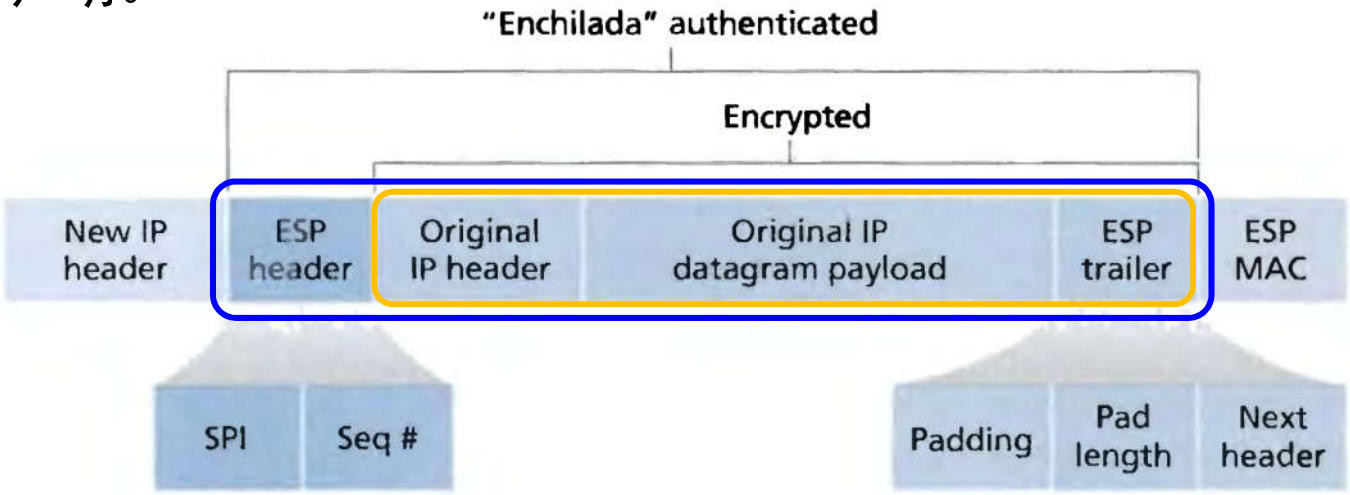
- **IPsec (ESP) Datagram in Tunnel Mode**
  - 装包过程
    2. 将原 IP 报文以及第1步得到的 ESP trailer 作为一个整体进行加密封装。具体的加密算法与密钥由 SA 给出。



4.2 IPSec

4.2.4 ESP Protocol

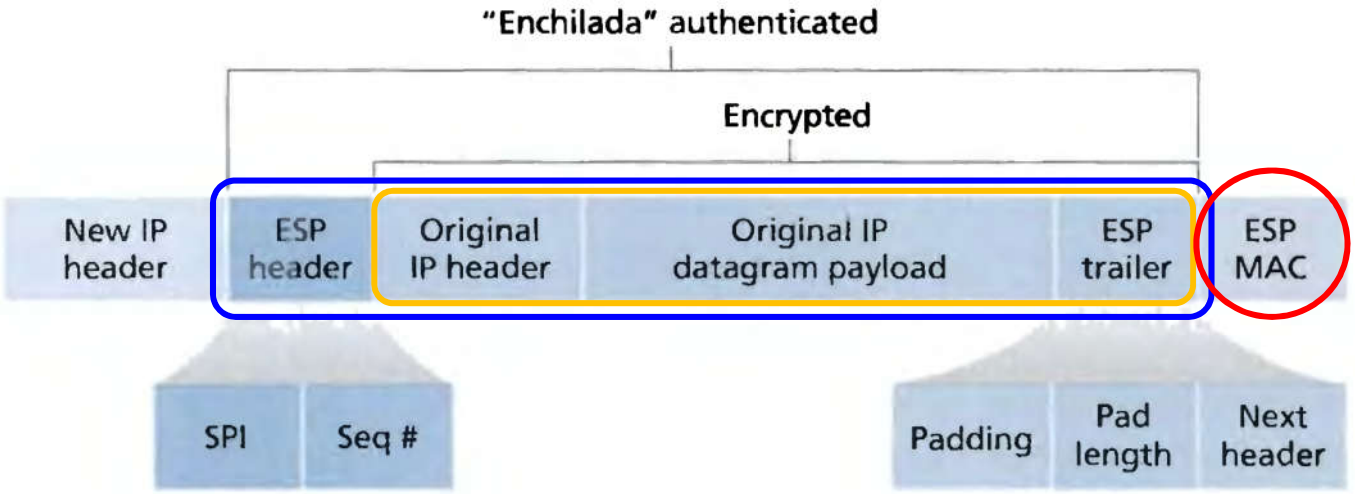
- **IPsec (ESP) Datagram in Tunnel Mode**
  - 装包过程
    3. 为第2步得到的加密数据添加 ESP header。ESP header由 SPI 和 Seq # 两部分组成。加密数据与 ESP header 合称为 “enchilada”，构成认证部分。注意到被封装的原报文的协议类型受到保护，没有在 ESP header 给出，而由加密的 ESP trailer 的 Next header 声明。



4.2 IPSec

4.2.4 ESP Protocol

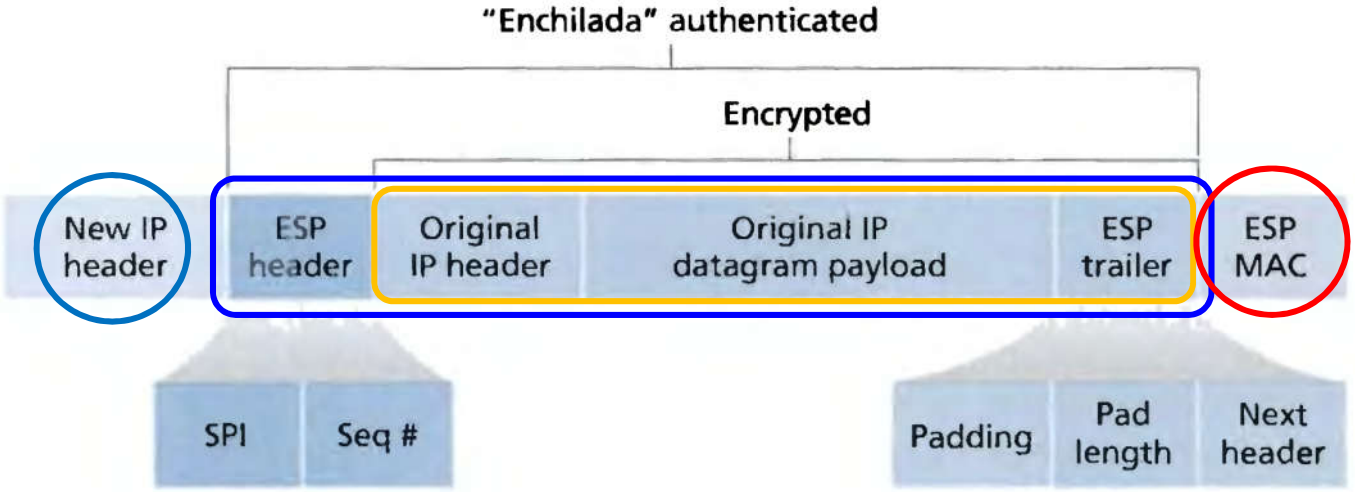
- **IPsec (ESP) Datagram in Tunnel Mode**
  - 装包过程
    4. 附加完整性度量结果 (ICV，Integrity check value)。对第3步得到的 “enchilada” 认证部分做摘要，得到一个32位整数倍的完整性度量值，并附在 ESP 报文的尾部。完整性度量算法包括验证密钥由 SA 给出。



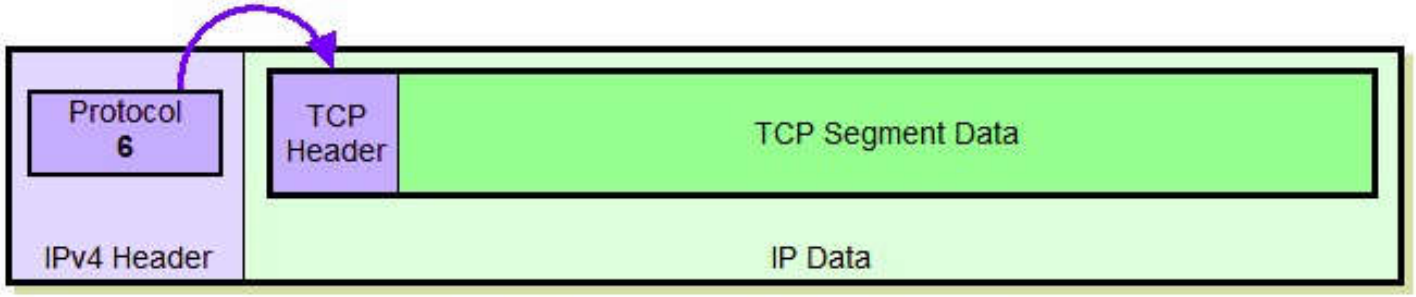
4.2 IPSec

4.2.4 ESP Protocol

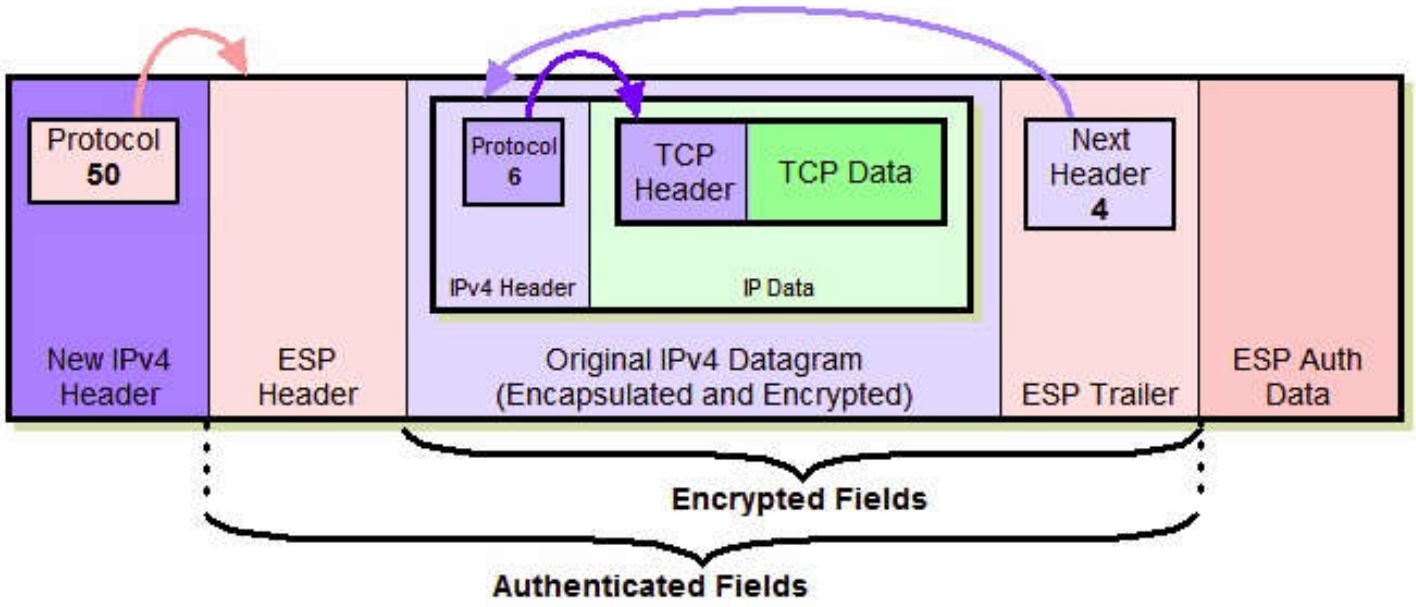
- **IPsec (ESP) Datagram in Tunnel Mode**
  - 装包过程
    5. 加上新的 IP header 构成 IPsec 报文。新构造的 IP header 附在 ESP 报文的前面组成一个新的 IP 报文。注意这个新的 IP header 的 IP 地址由路由器和安全网关解释，可以和原报文 (由主机创建的 IP 地址) 不同。协议类型为50，说明它封装的是一个 ESP 报文。



4.2 IPSec

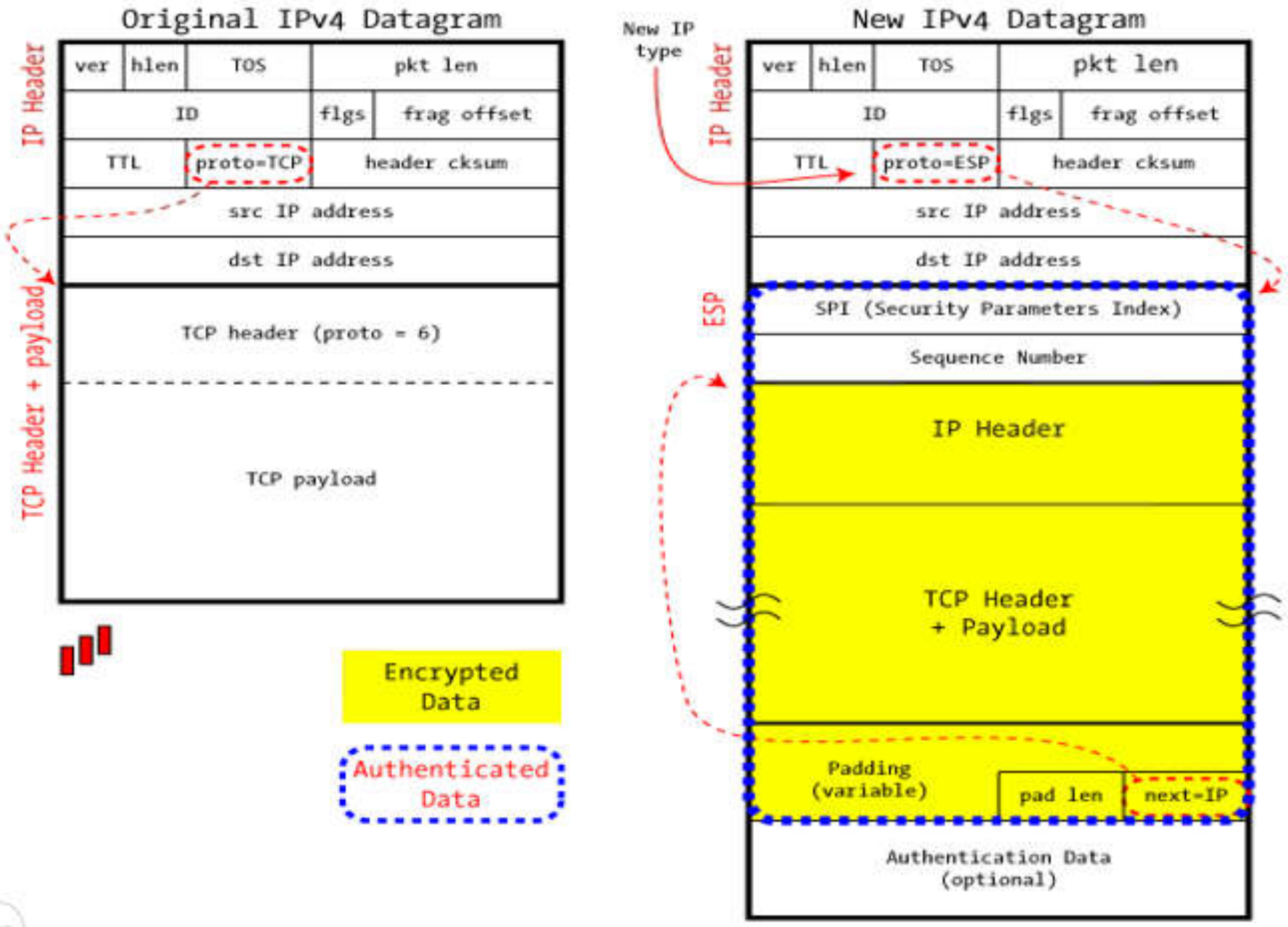


Original IPv4 Datagram Format



IPv4 ESP Datagram Format - IPSec Tunnel Mode

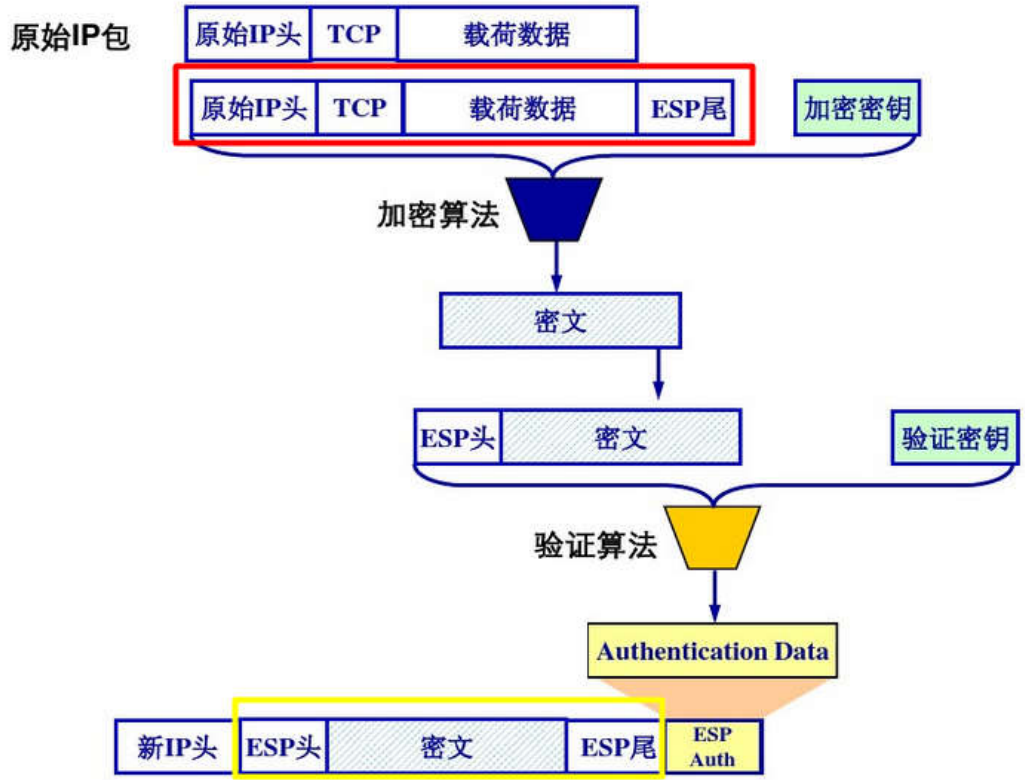
IPSec in ESP Tunnel Mode



4.2 IPSec

4.2.4 ESP Protocol

- **IPsec (ESP) Datagram in Tunnel Mode**
  - 隧道模式下的认证和传输区域
    - ✧ 红色区域是加密区域，黄色区域是验证区域。



4.2 IPSec

4.2.4 ESP Protocol

- **IPsec (ESP) Datagram in Tunnel Mode**
  - When a packet is received
    1. Use SPI to determine SA
    2. Calculate MAC
    3. Check sequence number
    4. Decryption
    5. Remove padding
    6. Forward the original datagram

4.2 IPSec

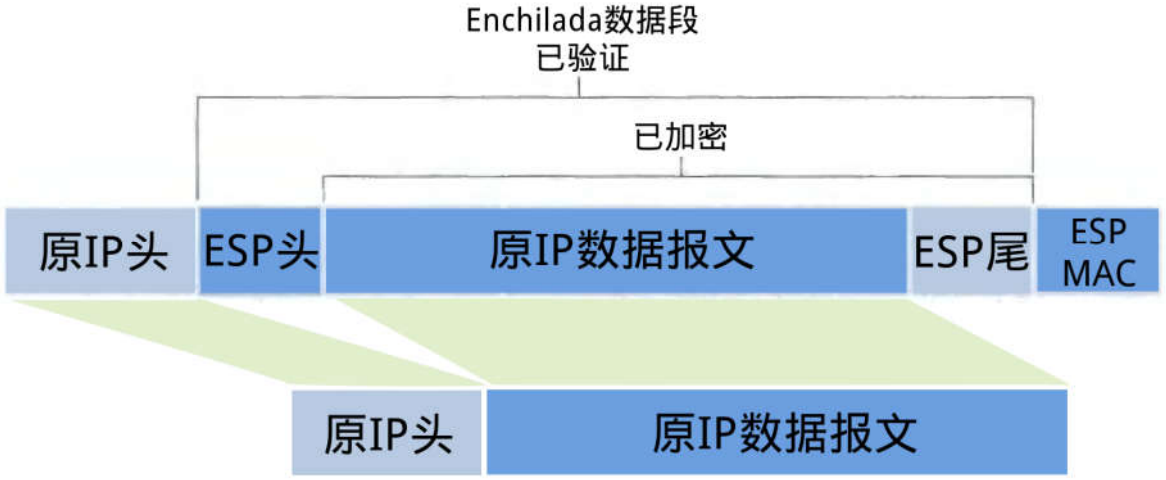
4.2.4 ESP Protocol

- **IPsec (ESP) Datagram in Tunnel Mode**
  - 拆包过程如下：
    1. 接收方收到 IP 报文后，发现协议类型是50，表明这是一个 ESP 包。首先查看 ESP header，通过 SPI 决定数据报文所对应的 SA，获得对应的模式 (tunnel/transport mode) 以及安全规范。
    2. 计算 “enchilada” 部分的摘要，与附在末尾的 ICV 做对比，验证数据完整性。
    3. 检查 Seq # 里的顺序号，保证数据是“新鲜”的。
    4. 根据 SA 所提供的加密算法和密钥，解密被加密过的数据，得到原 IP 报文与 ESP trailer。
    5. 根据 ESP trailer 的填充长度信息，找出填充字段的长度，删去后得到原来的 IP 报文。
    6. 最后根据得到的原 IP 报文的目的地址进行转发。

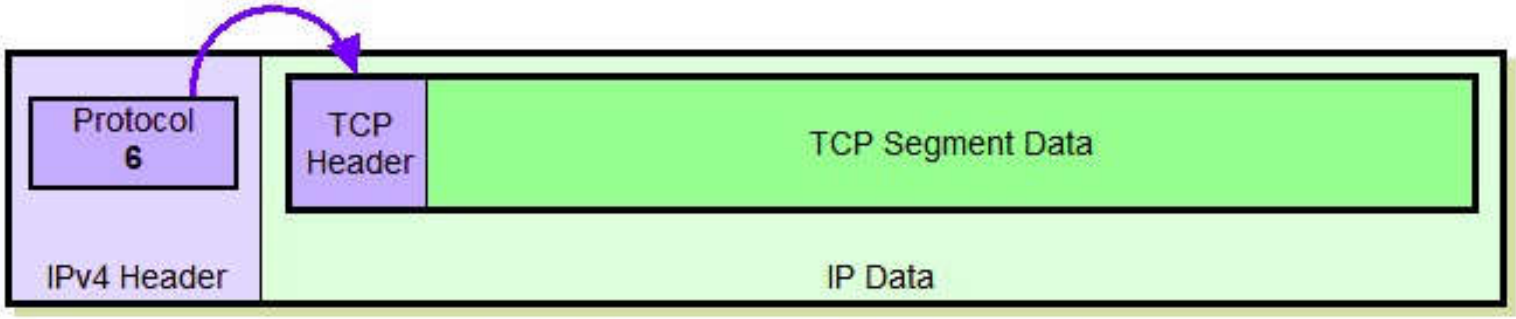
4.2 IPSec

4.2.4 ESP Protocol

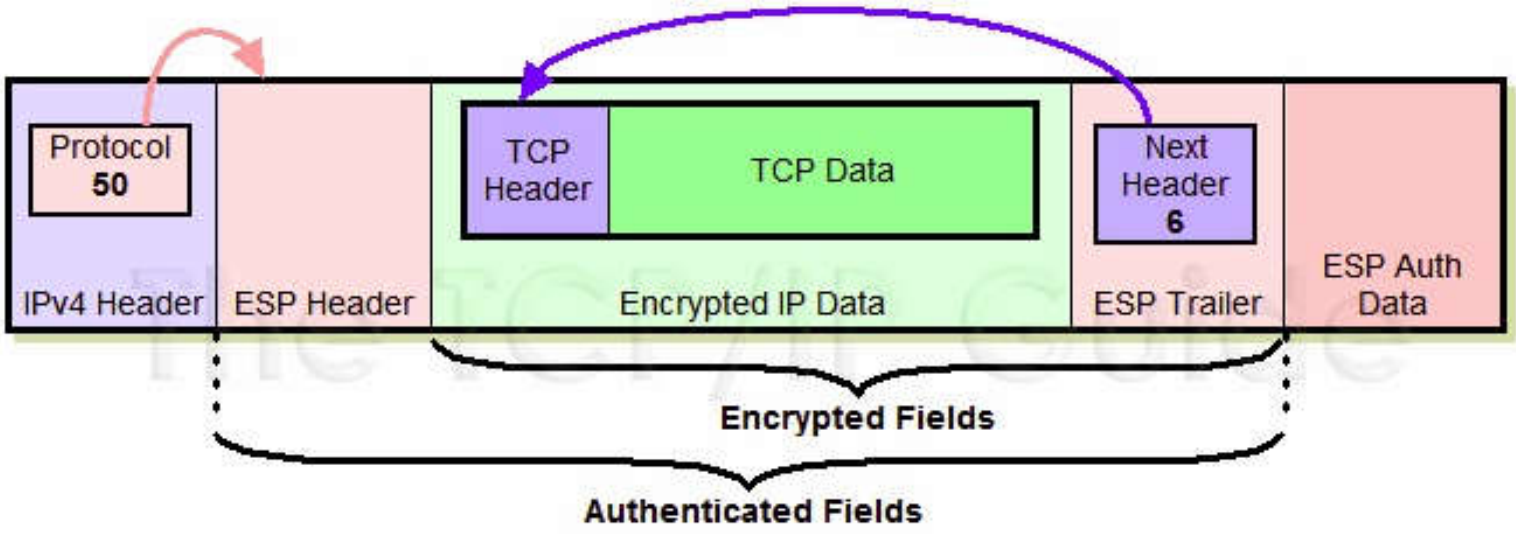
- **IPsec (ESP) Datagram in Transport Mode**



4.2 IPSec

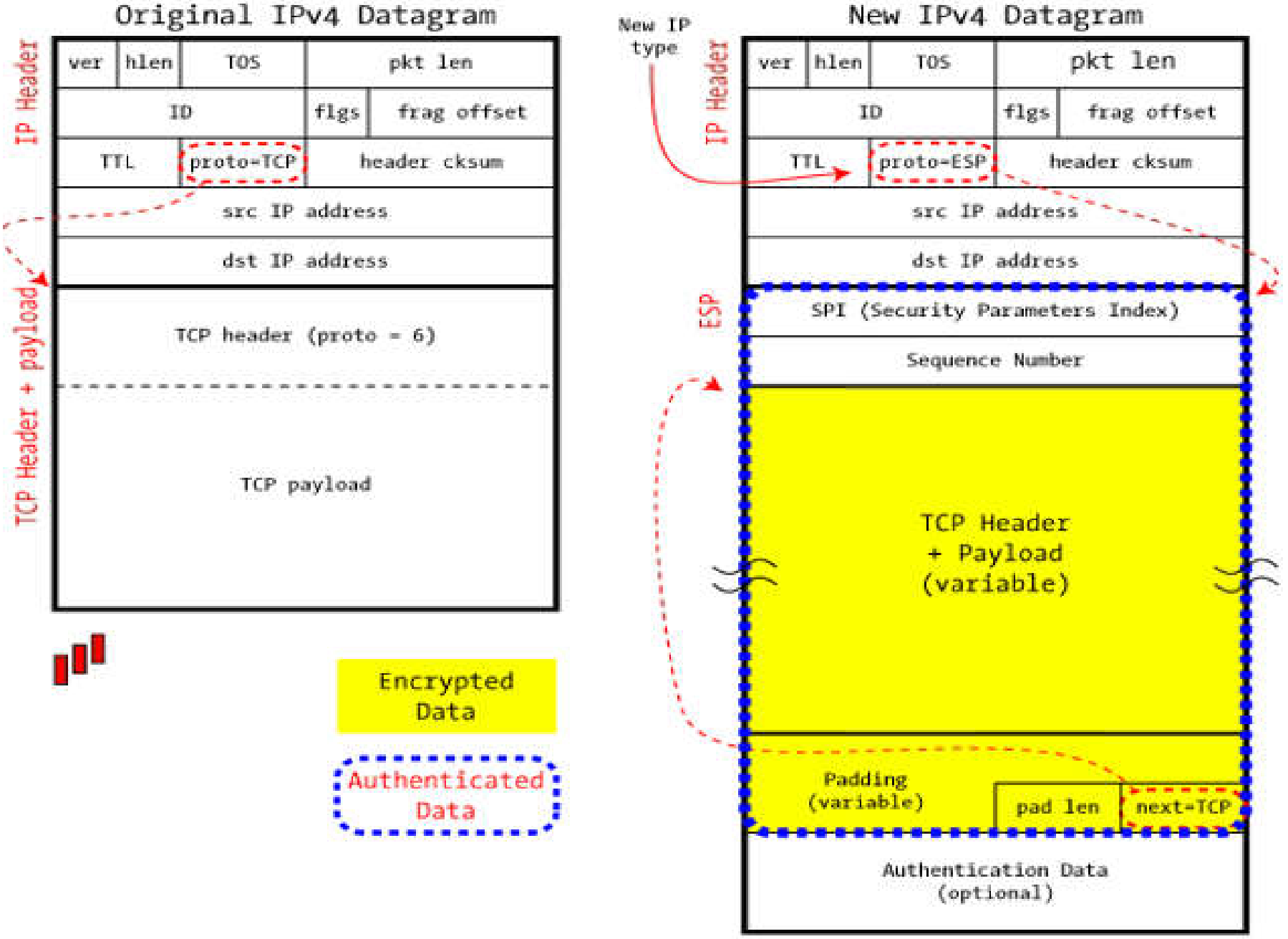


Original IPv4 Datagram Format



IPv4 ESP Datagram Format - IPSec Transport Mode

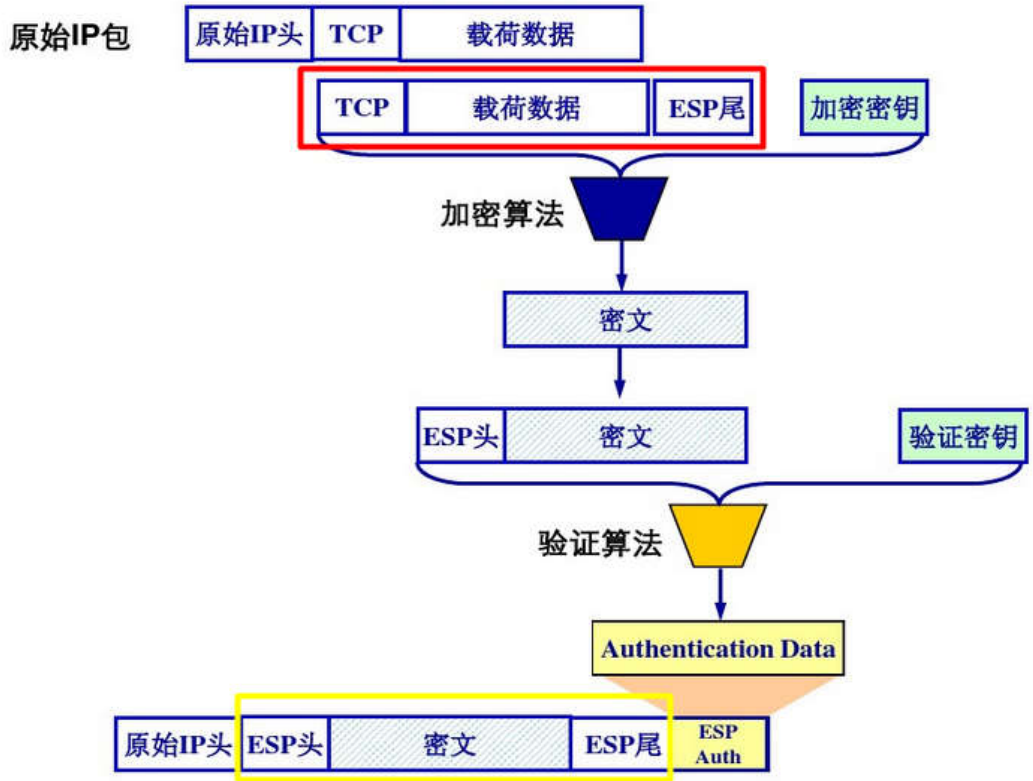
IPSec in ESP Transport Mode



4.2 IPSec

4.2.4 ESP Protocol

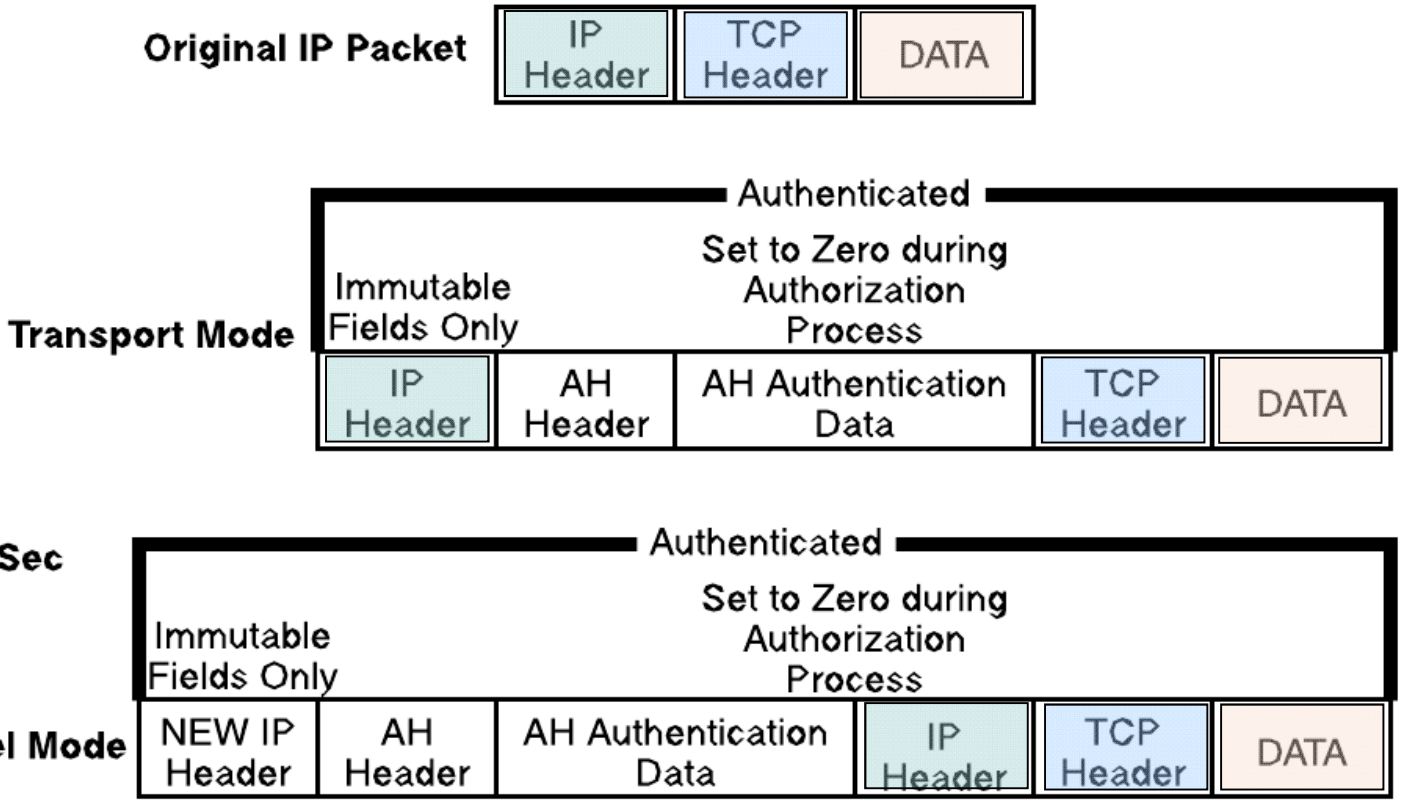
- **IPsec (ESP) Datagram in Transport Mode**
  - 传输模式下的认证和传输区域
    - ✧ 红色区域便是加密区，黄色区域是验证区。



4.2 IPSec

4.2.5 AH Protocol

- **A Brief Mention of AH Protocol**



4.2 IPSec

4.2.5 AH Protocol

- **A Brief Mention of AH Protocol**
  - AH 协议能够对数据进行完整性度量和来源认证，但不提供任何的加密服务，所以它只适用于数据不需要保密的情况。
  - AH 协议头结构：

0 7	8 15	16 31
Next Header	Payload Len	Reserved
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (Variable)		

4.2 IPSec

4.2.5 AH Protocol

- **A Brief Mention of AH Protocol**
  - Next Header 占8位，存放了连接在认证头后面的有效负载 (payload) 的类型。
  - Payload Len 指定 AH 的长度，具体的计算方法是以32位 为单位来表示 AH 的长度，再减去2。例如一段占64位的认证数据加上固定的96位协议头，一共是160位，那么，最终算出的 Payload Len 应是 [(96+64)/32]-2，即 3。
  - Reserved 占16位，为预留区域，方便以后扩充。目前应该全为0。这部分在计算认证数据时也会参与计算。

4.2 IPSec

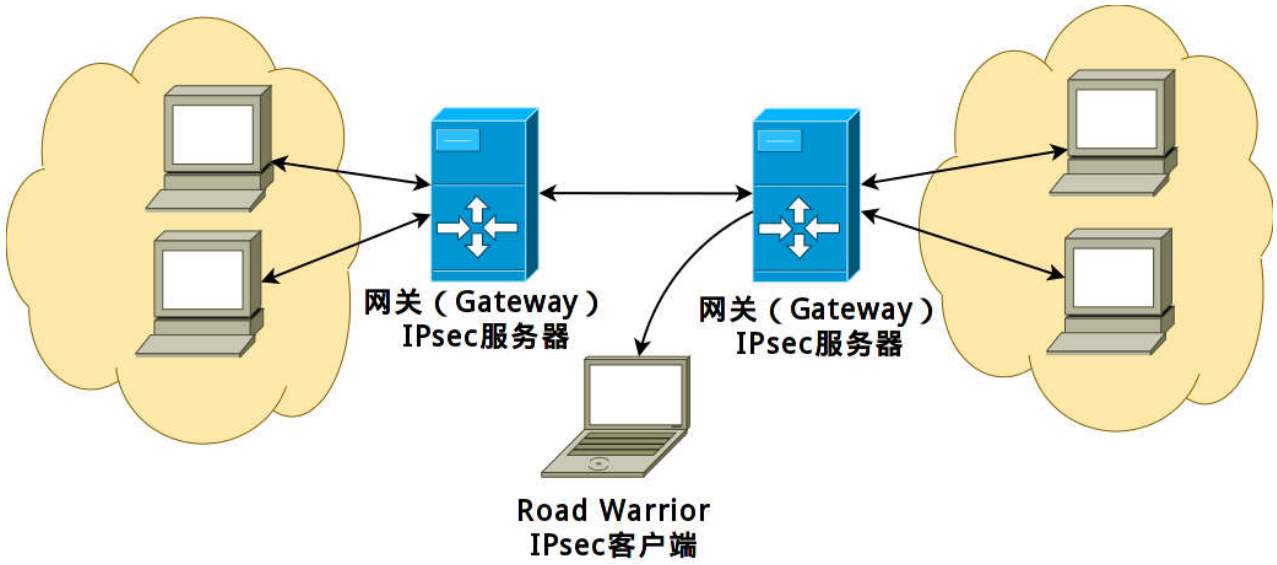
4.2.5 AH Protocol

- **A Brief Mention of AH Protocol**
  - SPI 占32位，用于将 AH 数据报文与相应的 SA 做映射。
  - Sequence Number Field 占32位，存放了一个递增的计数值，用于抵抗重放攻击。该字段是强制要求使用的，无论是否启用了反重放攻击的功能。当 SA 建立时置为0。
  - Authentication Data，认证数据，即报文的完整性度量值 (Integrity Check Value)。长度是可变的，但必须是32位的倍数，不足时需要填充。

4.2 IPSec

4.2.6 Gateway and Road Warrior Models

- **Gateway 模式和 Road Warrior 模式**
  - IPsec 通常应用于两种情况，一是两个私有网络通过因特网 的对接，另一种情况是外出办公的内部人员通过因特网连入私有网络，两者都需要保护好通信数据。如图所示：



4.2 IPSec

4.2.6 Gateway and Road Warrior Models

- **Gateway 模式和 Road Warrior 模式**
  - Gateway 模式是两个网关之间的通信，只需要在两边的网关上做好 IPsec 的设置。
  - Road Warrior 模式一头是网关，另一头是单个的客户端 (例如一台笔记本)。
    - ✧ 无论是 Gateway 模式还是 Road Warrior 模式，至少有一边是网关。想要通过 Internet 向网关后面某个内部主机发送信息时，需要先将经过 IPsec 保护的数据包发给网关，由网关将这个报文解包转发到真正的目的地。
  - 私有网络内的主机通常被认为是可信的，因此在一个私有网络内部，没有必要为每一台设备配置 IPsec，而只需要在私有网络对外的出口，即网关处配置。

4.2 IPSec

4.2.7 IKE – Key Management of IPsec

- **IKE (Internet Key Exchange)**
  - ISAKMP (RFC2408)
    - Internet security and key management protocol
      - Used for establishing Security Associations (SA) and cryptographic keys in an Internet environment. It only provides a framework for authentication and key exchange and is designed to be key exchange independent.
  - Oakley (Hilarie K. Orman, 1998)
    - The Oakley Key Determination Protocol
      - a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie–Hellman key exchange algorithm.
  - SKEME (Hugo Krawczik, 1996)
    - Secure Key Exchange Mechanism for Internet

4.2 IPSec

4.2.7 IKE – Key Management of IPsec

- **IKE (Internet Key Exchange)**
  - IPSec 的通信双方需要事先协商好将要采用的安全策略，包括使用的加密算法、密钥、密钥的生存期等，亦即创建 SA。AH 和 ESP 都需要使用 SA，而 IKE 的主要功能就是 SA 的建立和维护。
  - IPsec 使用 IKE (Internet Key Exchange) 协议来进行自动的密钥管理。IKE 实际上是一个混合协议，它包含协议
    - ISAKMP
    - Oakley
    - SKEME
  - ISAKMP 协议是 IKE 协议的主要组成部分，它负责指定密钥的协商过程。ISAKMP 协议只是一个框架，并未规定具体使用的加密算法。
  - Oakley 和 SKEME 协议可以理解为加密算法的具体规定。

4.2 IPSec

4.2.7 IKE – Key Management of IPsec

- **IKE (Internet Key Exchange)**
  - 使用 IKE 的 IPsec 的密钥协商分为两个阶段：
    - ✧ 阶段一：建立 IKE-SA。
      - ◌ 双方使用 *Diffie-Hellman* 算法创建两个方向的 IKE-SA，这里的 IKE-SA 与前面讲的 SA 有所不同。事实上通信时只有一个 IKE-SA 被建立，由通信的两个方向共享。期间还会生成阶段二协商所需用到的密钥。
    - ✧ 阶段二：协商 IPsec SA。
      - ◌ 阶段二又称为快速模式 (quick mode)。阶段二的协商在阶段一所建的安全信道中进行，例如选用 ESP 还是 AH，加密用的密钥等等。 从这一阶段起后面的数据都是经过加密的。

4.2 IPSec

4.2.7 IKE – Key Management of IPsec

- **IKE (Internet Key Exchange)**
  - 第一阶段可细分为主模式和激进模式。
    - ✧ 主模式 (Main Mode)；激进模式 (Aggressive Mode)。
    - ✧ 主模式需要进行多次数据交换，在交换密钥后对双方的身份消息进行加密，防止中间人攻击。虽然速度慢，但更安全。激进模式需要较少的数据交换，速度更快，但安全性有所降低。
  - Note.
    - ✧ The ***Diffie–Hellman*** key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
      http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

End of Chapter 4.2