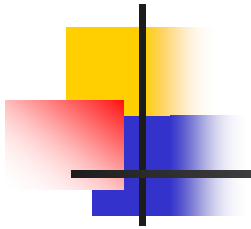
宽带通信网

信息与通信工程学院

靳浩

宽带通信网

- 通信网技术发展概述
- ATM 技术原理
- ATM的流量控制和拥塞控制技术
- 宽带网交换技术
- IP网络体系结构与关键技术
- IP网络的QOS技术
- IP网络安全与管理技术
- MPLS技术及其发展
- 移动IP技术及其发展
- 下一代网络技术



IP网络安全与管理技术

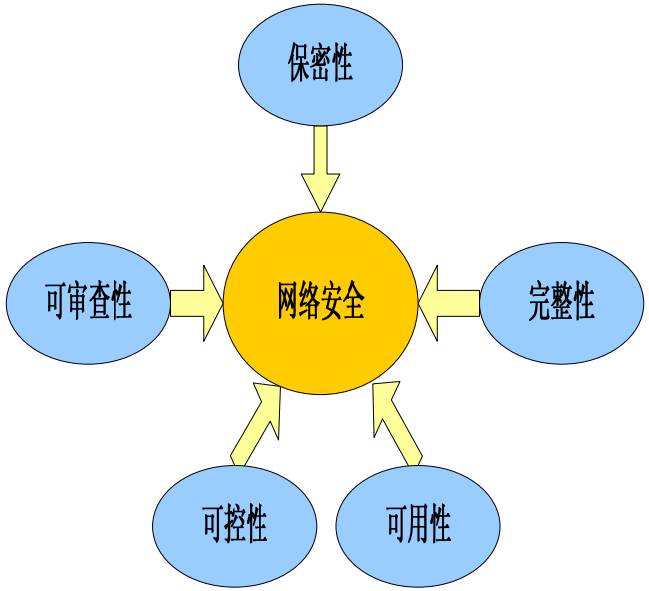
- 网络安全的概念
- 网络安全的属性
- 引起网络不安全的因素
- 安全协议

网络安全的概念

- 网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。
- 网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全的属性

- 保密性:信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。
- 可控性：对信息的传播及内容具有控制能力。
- 不可否认性（可审查性）：指信息的行为人要对自己的信息行为负责，不能抵赖自己曾作出的行为，也不能否认曾经接到对方的信息。出现安全问题时提供审查的依据与手段。



引起网络不安全的因素

- 操作系统的脆弱性
  - 操作系统其体系结构本身可能就是一种不安全的因素；
  - 由于操作系统可以创建进程，即使在网络的节点上同样也可以进行远程进程的创建与激活，而且被创建的进程具有可以继续创建过程的权力；
  - 网络操作系统提供的远程过程调用（RPC）服务以及它所安排的无口令入口也常常是黑客的入侵通道。
- 计算机系统的脆弱性
  - 存在超级用户，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者；
  - 计算机可能会因硬件或软件故障而停止运转，或被入侵者利用并造成损失；
  - 计算机系统上运行的软件本身存在安全漏洞。

引起网络不安全的因素

- 协议安全的脆弱性
  - 当前计算机网络系统都使用的TCP/IP协议以及FTP、E-mail、NFS等都包含着许多影响网络安全的因素，存在许多漏洞；
  - 黑客通常采用Sock、TCP预测或使用远程访问（RPC）进行直接扫描等方法对防火墙进行攻击；
- 数据库管理系统安全的脆弱性
  - 由于数据库管理系统（DBMS）对数据库的管理是建立在分级管理的概念上的，因此DBMS的安全也存在隐患；
  - DBMS的安全必须与操作系统的安全配套，由于操作系统本身也存在安全隐患，所以这是DBMS一个先天的不足之处。

引起网络不安全的因素

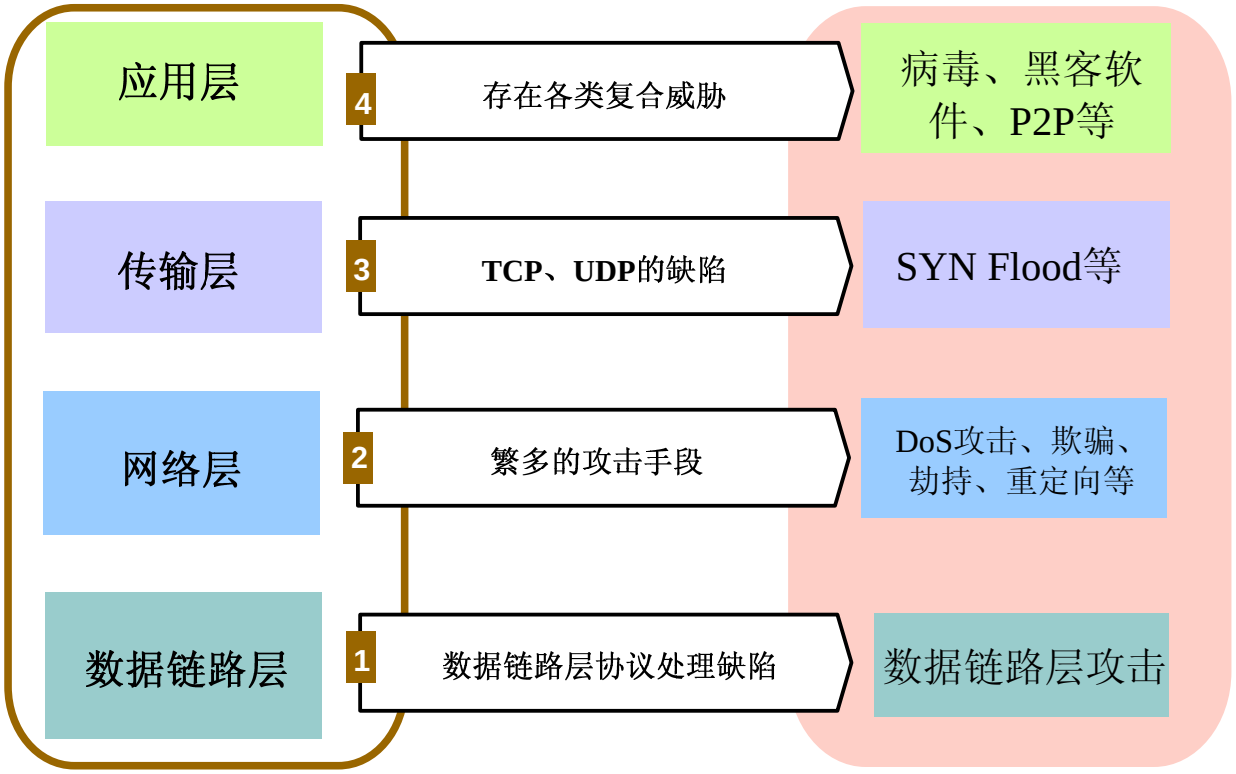
- 管理的因素
  - 不管是什么样的网络系统都离不开人的管理，但又大多数缺少安全管理员，特别是高素质的网络管理员；
  - 缺少网络安全管理的技术规范，缺少定期的安全测试与检查，更缺少安全监控，比如许多网络系统已使用多年，但网络管理员与用户的注册名或口令等还处于缺省状态。
- 其他各种外部因素
  - 网络设备所存放的环境安全因素，比如电源的健壮性，环境的温度、湿度、洁净程度以及防雷、防静电、防水、防火、防电磁干扰等是否符合要求；
  - 物理链路工作不正常遭受意外破坏，包括人为和自然的破坏。

网络安全面临的威胁

- 网络安全面临的威胁包括人为威胁和自然威胁和人为威胁，其中人为威胁最严重，包含：
  - 非授权访问:这主要的是指对网络设备以及信息资源进行非正常使用或超越权限使用;
  - 假冒合法用户:主要指利用各种假冒或欺骗的手段非法获得合法用户的使用权，以达到占用合法用户资源的目的;
  - 数据完整性受破坏，或数据发生泄露;
  - 干扰网络的正常运行，更改网络运行参数;
  - 由病毒引发的不良后果.

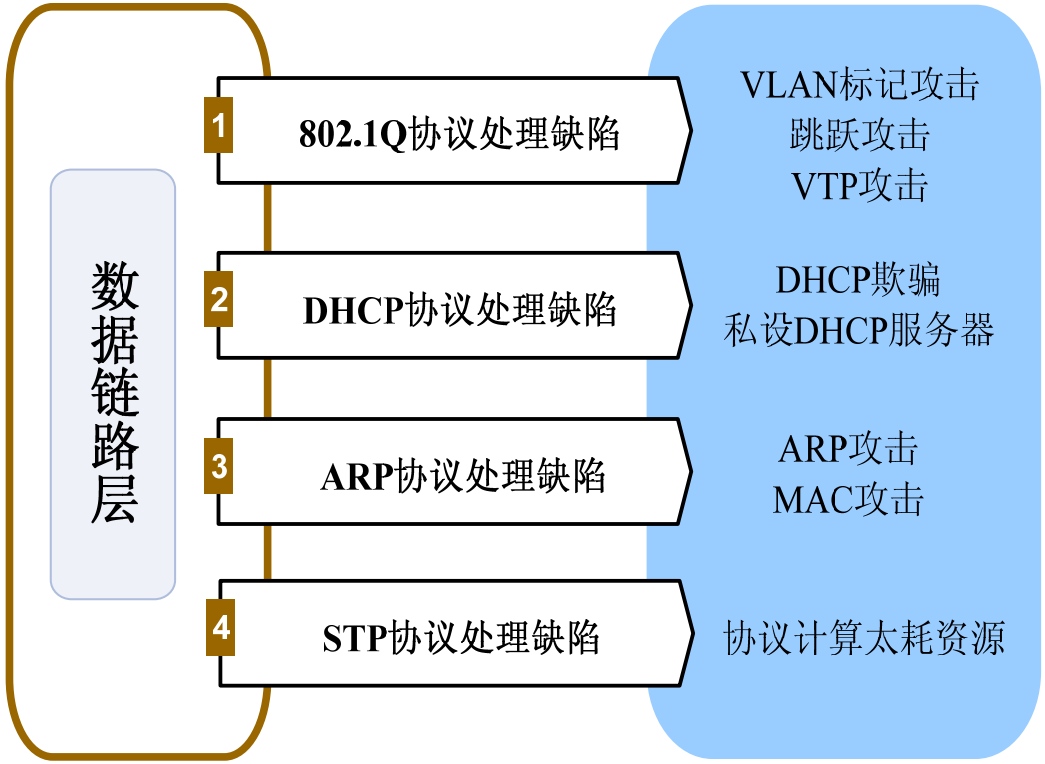
TCP/IP协议中的网络安全威胁

- TCP/IP协议中的网络安全威胁包括来自数据链路层、网络层、传输层和应用层的安全威胁。



数据链路层安全威胁

- 与VLAN相关的威胁
- MAC攻击威胁
- DHCP攻击威胁
- ARP攻击威胁
- 生成树协议攻击威胁



网络层安全威胁

- 资源耗竭型攻击：DoS攻击，主要以使设备停止服务性功能为目的。
- 欺骗攻击：伪造数据包进行攻击，如伪造源IP地址等来获取某些权限。
- 对传输层的攻击：阻隔上层协议和主机之间的交互，采用会话劫持来获取权限，或窃听数据、伪造数据注入。
- 对路由协议的攻击：阻断路由器和新老邻居对等体之间的交互、重定向流量、注入虚假信息等来阻断用户合法的数据流。

网络层安全威胁

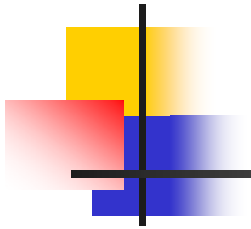
- 针对控制层面的IP服务的攻击：如针对DHCP、DNS、NTP等的攻击，影响它们的正常工作。
- 未授权接入攻击：试图对受限系统进行非授权接入的攻击。
- 利用软件弱点的攻击：如果软件的弱点被利用，会对路由器的机密性、完整性和可用性造成极大危害，也会影响数据层面的流量。
- 恶意的网络探测：对目标进行信息收集，以期找寻系统的弱点或漏洞，为将来可能的攻击做准备。

传输层安全威胁

- 针对传输层的威胁主要是用于影响TCP和UDP协议的，常见的威胁有：
  - TCP SYN flooding：向目的主机发送大量的TCP SYN，而不回应TCP ACK，使大量连接处于半开状态（half-open），导致预留资源长时间不能释放（直到超时），最终致使目的端资源耗尽。
  - UDP flooding：利用了UDP传输的无状态性，通过发送大量拥有伪装IP地址的UDP数据包，填满网络设备（主要是路由器或防火墙）的连接状态表，造成服务被拒绝。
  - Crikey CRC flooding：目标主要是防火墙等纪录连接状态的网络安全设备。为了加速数据包通过防火墙，防火墙通常不会使用 Checksum 对数据包进行效验，只是把连接添加到连接状态表中；Crikey CRC flooding在TCP和UDP头部加入错误的Checksum值。当这些数据包到达目的主机时，因为Checksum错误会被拒绝。这样，实际上没有 建立起来的连接被纪录到了连接状态表中，如果防火墙大量接受到这样的数据包，最终会导致连接状态表被填满，新的连接请求被拒绝。

应用层安全威胁

- 常见的属于应用层的协议有：简单邮件传输协议（SMTP），文件传输协议（FTP），超文本传输协议（HTTP），远程连接服务标准协议（TELNET），简单网络管理协议（SNMP）以及域名系统（DNS）.
  - 带宽滥用：主要表现为P2P和即时通讯软件消耗了大量带宽，轻则影响企业业务无法正常运作，重则致使企业IT系统瘫痪。
  - 大量的带宽浪费在与工作无关流量上，造成了投资的浪费和效率的降低。另一方面，P2P使得文件共享和发送更加容易，带来了潜在的信息安全风险。
  - 德国互联网调研机构ipoque称，P2P已经彻底统治了当今的互联网，其中50-90%的总流量都来自P2P程序。



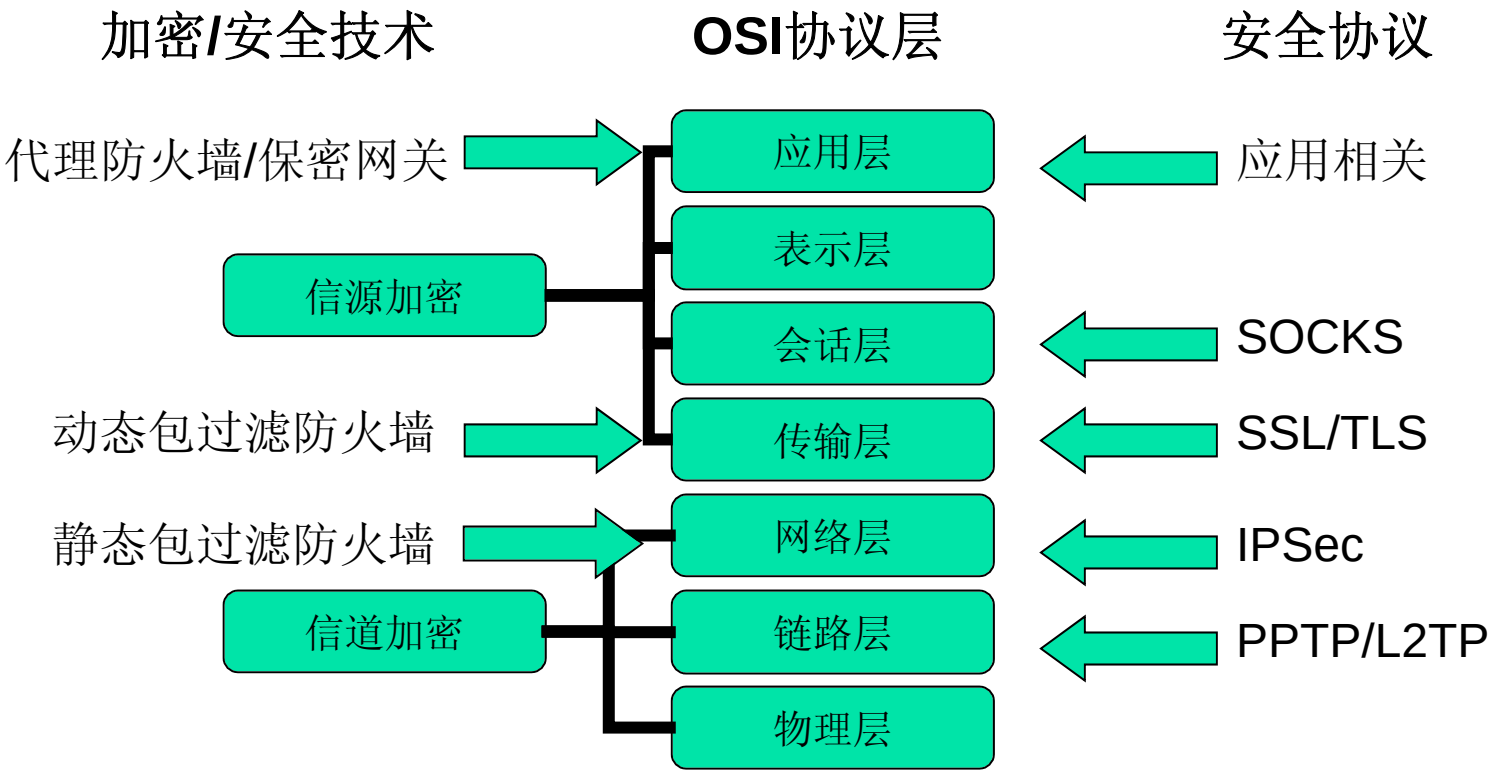
安全协议

- 安全协议概述
- 应用层安全协议
- 传输层安全协议
- 网络层安全协议

安全协议概述

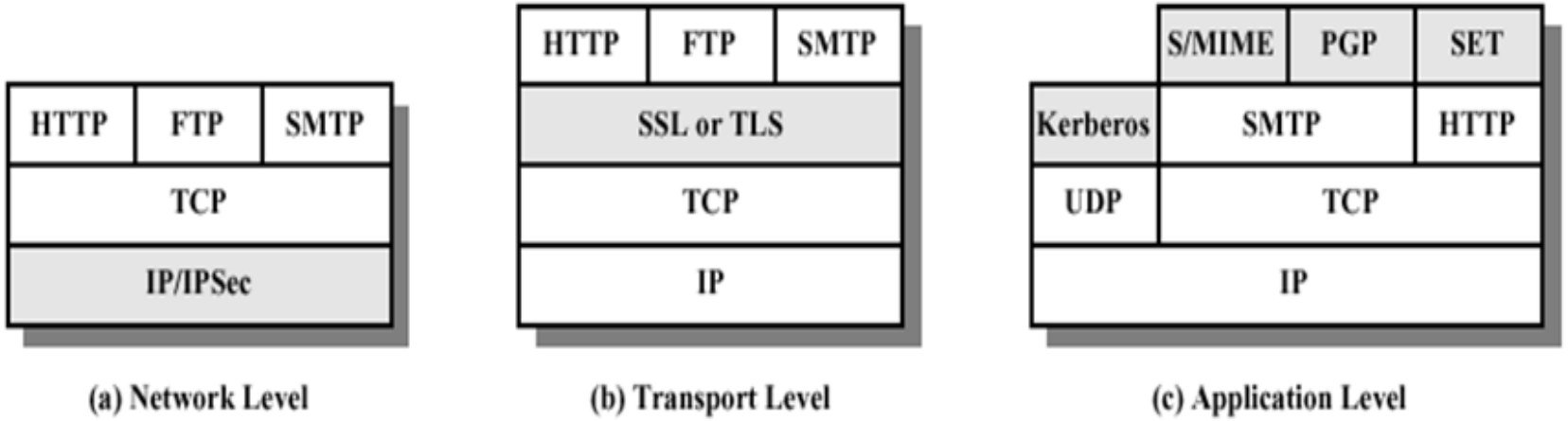
- 安全协议本质上是关于某种应用的一系列规定，包括功能、参数、格式、模式等，通信各方只有共同遵守协议才能互相操作。
- 在信息网络中，可以在ISO七层协议中的任何一层采取安全措施，大部分安全措施都采用特定的协议来实现，如：
  - 网络层加密和认证采用IPSec协议；
  - 传输层加密和认证采用SSL协议等。

OSI协议层

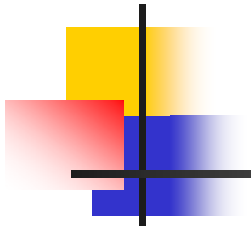


OSI七层协议与信息安全

TCP/IP协议栈中的安全



Relative Location of Security Facilities in the TCP/IP Protocol Stack



应用层安全协议

- SSH
- SET
- S-HTTP
- PGP
- S/MIME

SSH

- 在实际工作中，SSH（Secure Shell）协议通常是替代TELNET协议、RSH协议来使用的。它类似于TELNET协议，允许客户机通过网络连接到远程服务器并运行该服务器上的应用程序，被广泛用于系统管理中。
- 该协议可以加密客户机和服务器之间的数据流，这样可以避免TELNET协议中口令被窃听的问题。该协议还支持多种不同的认证方式，及用于加密包括FTP数据外的多种情况。

SET

- SET (安全电子交易) 协议是电子商务中用于安全电子支付最典型的代表协议。
- 是由MasterCard和VISA制定的标准，这一标准的开发得到了IBM、Microsoft、Netscape、SAIC、Terisa 和 Verisign 的投资以及其他信用卡和收费卡发行商的支持。
- SET是在一些早期协议(SEPP、VISA、STT)的基础上整合而成的，它定义了交易数据在卡用户、商家、发卡行、收单行之间的流通过程，以及支持这些交易的各种安全功能(数字签名、Hash算法、加密等)。

S-HTTP

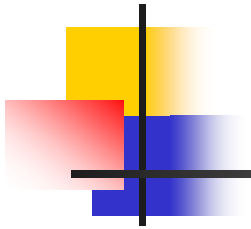
- WWW是在超文本传输协议(HTTP)基础上建立起来的，但HTTP中不包含安全性机制，因此提出了安全HTTP(S-HTTP)。
- S-HTTP是对HTTP的扩展，描述了一种使用标准加密工具来传送HTTP数据的机制。
- S-HTTP工作在应用层，同时对HTML进行了扩展，服务器方可以在需要进行安全保护的文档中加入加密选项，控制对该文档的访问及加密、解密、签名算法等。
- 由于缺乏厂商的支持，S-HTTP协议现在已经几乎不再使用。

PGP

- PGP (Pretty Good Privacy)主要用于安全电子邮件，它可以对通过网络进行传输的数据创建和检验数字签名、加密、解密以及压缩。
- 除电子邮件外，PGP还被广泛用于网络的其他功能之中。
- PGP的源代码免费使用、完全公开。

S/MIME

- S/MIME是在MIME(多用途Internet邮件扩展)规范中加入了获得安全性的一种方法，提供了用户和认证的形式化定义，支持邮件的签名和加密。

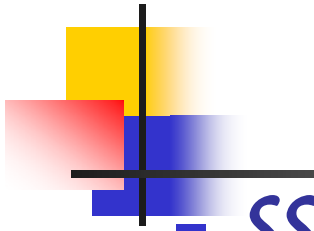


传输层安全协议

- SSL/TLS
- PCT

SSL/TLS

- 1994年Netscape开发了SSL(Secure Socket Layer)协议，专门用于保护Web通信。
- SSL/TLS的版本和发展历史
  - SSL1.0，不成熟；
  - SSL2.0，基本上解决了Web通讯的安全问题；
    - Microsoft公司发布了PCT(Private Communication Technology)，并在IE中支持；
  - SSL3.0，1996年发布，增加了一些算法，修改了一些缺陷；
  - TLS 1.0(Transport Layer Security，也被称为SSL 3.1)，1997年IETF发布了Draft，同时，Microsoft宣布放弃PCT，与Netscape一起支持TLS 1.0；
  - 1999年，发布RFC 2246(The TLS Protocol v1.0)。



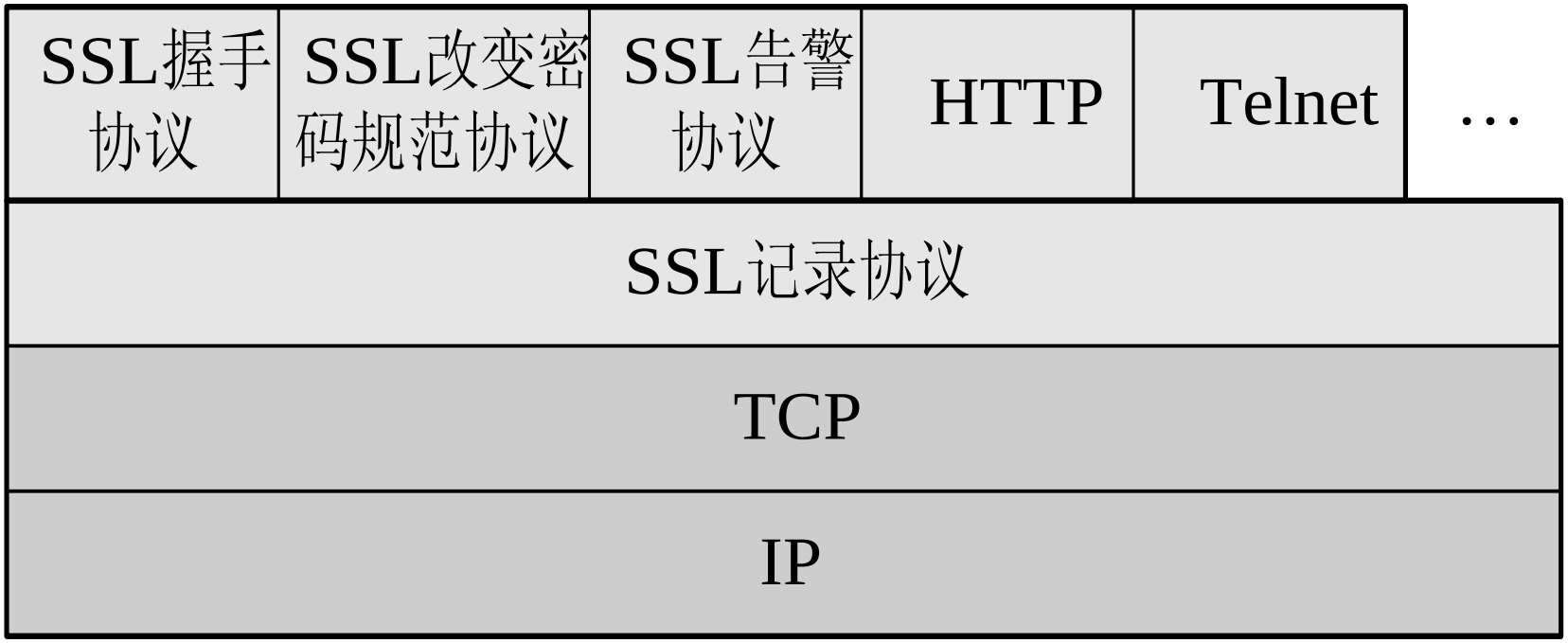
SSL

- SSL协议概述
- SSL协议体系结构
- SSL记录协议
- SSL改变密码规范协议
- SSL告警协议
- SSL握手协议

SSL协议概述

- SSL(安全套接字层，Secure Socket Layer)是由Netscape开发的安全协议。它工作在传输层，独立于上层应用，为应用提供一个安全的点对点通信隧道。
- SSL由多个协议组成，采用两层协议体系结构。
- 功能：在客户端和服务器之间提供安全通信，允许双方互相认证、使用消息的数字签名来提供完整性、通过加密提供消息保密性。

SSL协议体系结构



SSL协议体系结构

- SSL由协商过程和通信过程组成，其中
  - 协商过程用于确定加密机制、加密算法、交换会话密钥服务器认证以及可选的客户端认证；
  - 通信过程秘密传送上层数据。

SSL协议体系结构

- 客户和服务器之间需要交换信息，以便完成以下功能：
  - 认证服务器身份；
  - 认证客户端身份；
  - 使用公钥加密技术产生共享秘密信息；
  - 建立加密的SSL连接。

SSL协议体系结构

- SSL记录协议：规定了数据传输格式；
- SSL握手协议：使得服务器和客户能够相互认证对方的身份，协商加密和MAC(消息认证码)算法以及用来保护SSL记录中发送的数据的加密密钥，可以支持众多加密、哈希和签名算法；
- SSL改变密码规范协议；
- SSL告警协议；

SSL的工作机理

- SSL协议在工作过程中需要建立SSL会话和SSL连接：
  - 连接：连接是能够提供合适服务类型的传输。对SSL，这种连接是对等的、暂时的，每个连接都和一个会话相关；
  - 会话：SSL会话是指客户机和服务器之间的关联，会话由握手协议创建；会话定义了一组可以被多个连接共用的密码安全参数；
  - 对于每个连接，可以利用会话来避免对新的安全参数进行代价昂贵的协商。

SSL的工作机理

- 在任意通信双方之间(例如在客户机和服务器上的HTTP应用程序)，可能有多个安全连接。理论上，双方可以存在多个同时的会话，但在实际中大都是一对一关系；
- 一个SSL会话是有状态(Stateful)的，由SSL握手协议负责协调客户机和服务器之间的状态；
- SSL会话逻辑上有两种状态，一个是当前操作状态，另外一个是(在握手协议期间)未决状态。此外，还需维持独立的读和写状态。

SSL的工作机理

- 当客户机或者服务器接收到改变码规范消息时，它就会拷贝未决读状态为当前读状态；
- 当客户机或者服务器发送一条改变密码规范消息时，它就会拷贝未决写状态为当前写状态；
- 当握手协商完成时，客户机和服务器交换改变密码规范消息，然后它们之间的后续通信采用新近达成的密码规范进行处理。

SSL会话状态包含的元素

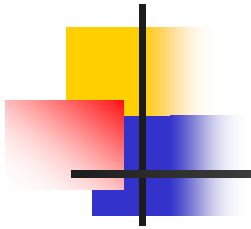
- 会话标识符(Session Identifier)：是指服务器选择的用来识别一个激活的或可恢复的会话状态的一个任意字节序列；
- 对等实体证书(Peer Certificate)：X509.v3证书，该元素状态可为空；
- 压缩方法(Compression Method)：压缩数据的算法；
- 密码规范(Cipher Spec)：制定了分组数据加密算法(例如，null，DES等)以及MAC算法(例如，MD5或SHA)。同样还定义了密码属性，例如哈希长度；
- 主秘密(Master Secret)：客户机和服务器共享的48字节共享秘密；
- 是否可恢复(Is Resumable)：确定该会话是否可用于发起新连接的标志。

SSL连接状态包含的元素

- 服务器和客户机随机数(Server and Client Random)：服务器和客户机为每个连接选择的字节序列；
- 服务器写MAC秘密(Server Write MAC Secret)：服务器所写数据的MAC操作秘密；
- 客户机写MAC秘密(Client Write MAC Secret)：客户机所写数据的MAC操作秘密；
- 服务器写密钥(Server Write Key)：服务器加密数据和客户机解密数据的分组密码密钥；
- 客户机写密钥(Client Write Key)：客户机加密数据和服务器解密数据的分组密码密钥。

SSL连接状态包含的元素

- 初始化向量(Initialization Vectors)：当使用CBC模式的分组密码时，每个密钥都需要一个初始化向量，该域首次由SSL握手协议初始化，其后每条记录的最后密文块保留作为下一条记录的IV；
- 序列号(Sequence Numbers)：对于每次连接，双方都各自维护自己的序列号用于传输和接收的消息。每当某一方发送或者接收一条改变密码规范消息，都将把序列号设成零。序列号的类型为uint64，其值不能超过$2^{64}-1$。



SSL记录协议

- SSL协议的底层是记录协议层。SSL记录协议在客户机和服务器之间传输应用数据和SSL控制数据，其间有可能对数据进行分段或者把多个高层协议数据组合成单个数据单元。
- 最多能传送16384个字节的数据块。

SSL记录协议的工作机理

- SSL记录协议的整个操作过程
  - 第一步：分段过程。每一个高层消息都要分段，使其长度不超过214字节。
  - 第二步：选择是否进行压缩。目前的版本没有指定压缩算法，但压缩必须是无损的，而且不会增加1024字节以上长度的内容。一般我们总希望压缩是缩短了数据而不是扩大了数据，但是对于非常短的数据块，由于格式原因，有可能压缩算法的输出长于输入。

SSL记录协议的工作机理

- SSL记录协议的整个操作过程
  - 第三步：是给压缩后的数据计算消息验证码，MAC算法使用下面公式进行计算：

hash(MAC_write_secret + pad_2 +

hash(MAC_write_secret+pad_1+
seq_num+SSLCompressed.type+
SSLCompressed.length
+SSLCompressed.fragment));

("+"代表连接操作)

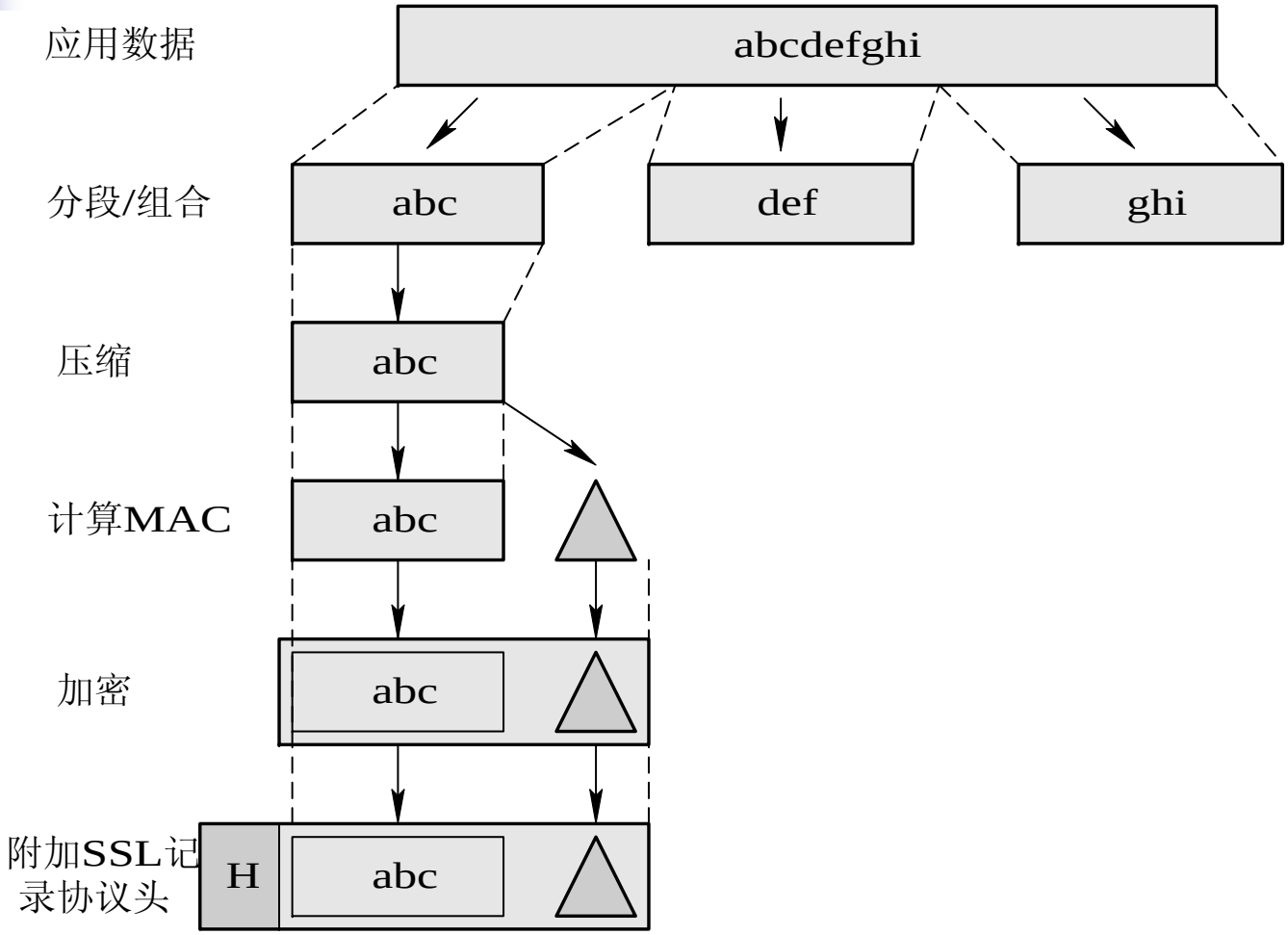
SSL记录协议的工作机理

- 各操作的含义
  - MAC_write_secret为客户服务器共享的秘密；pad_1为字符0x36重复48次(MD5)或40次(SHA)；
  - pad_2为字符0x5c重复48次(MD5)或40次(SHA)；
  - seq_num为消息序列号；
  - hash为哈希算法；
  - SSLCompressed.type为处理分段的高层协议类型；
  - SSLCompressed.length为压缩分段的长度；
  - SSLCompressed.fragment为压缩分段(没有压缩时，就是明文分段)。
- MAC运算要先于加密运算进行；
- 接着，使用对称加密算法给添加了MAC的压缩消息进行加密，加密不能增加1024字节以上的内容长度。

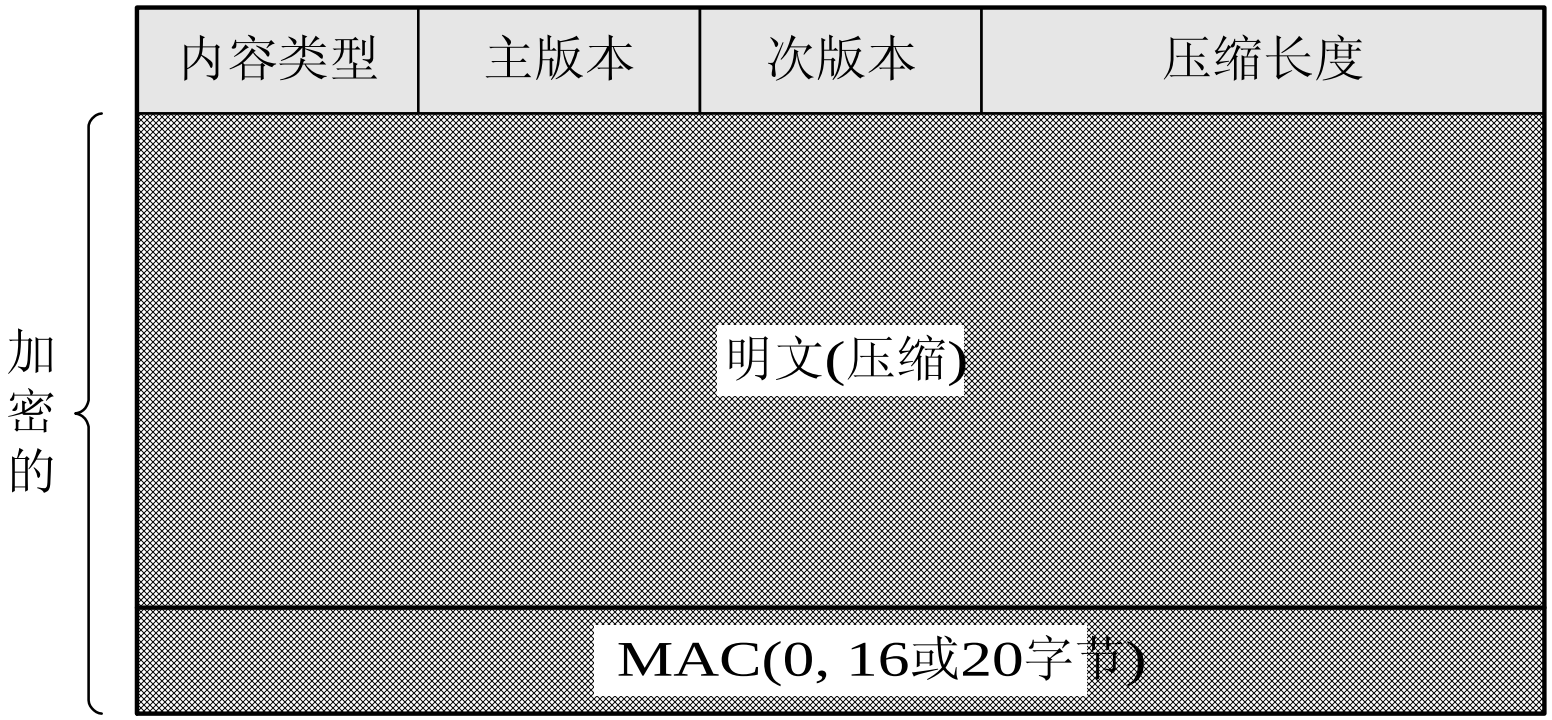
SSL记录协议的工作机理

- 实现SSL记录协议的最后一步是添加报头，它包含以下字段：
  - 内容类型(8位)：所封装分段的高层协议类型；
  - 主版本(8位)：使用SSL协议的主要版本号，对SSLv3值为3；
  - 次版本(8位)：使用SSL协议的次要版本号，对SSLv3值为0；
  - 压缩长度(16位)：分段的字节长度，不能超过214+2048。

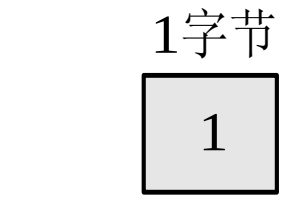
SSL记录协议的封装过程



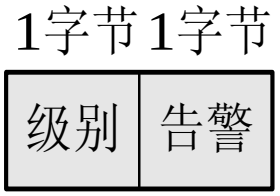
SSL记录头格式



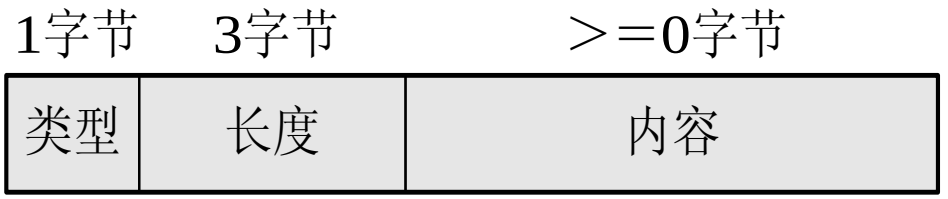
SSL记录协议的有效负载



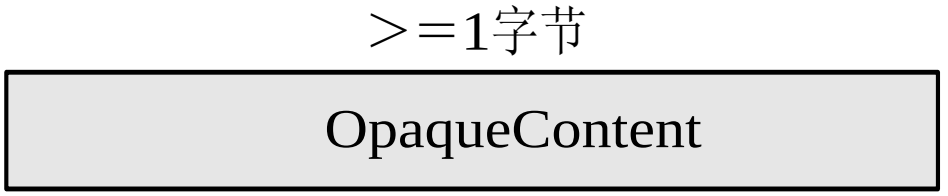
(a) 改变密码规范协议



(b) 告警协议



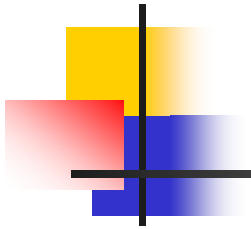
(c) 握手协议



(d) 其它上层协议

SSL握手协议

- SSL握手协议允许客户和服务器相互验证、协商加密和MAC算法以及保密密钥，用来保护SSL记录发送的数据；
- 握手协议通过一系列客户机和服务器的交换消息来实现；
- 客户端和服务器端的握手由以下几部分组成：
  - 协商数据传送期间使用的密码组(Cipher Suite)；
  - 建立和共享客户与服务器之间的会话密钥；
  - 客户认证服务器(可选)；
  - 服务器认证客户(可选)。



SSL改变密码规范协议

- 改变密码规范协议用于从一种加密算法转变为另外一种加密算法。
- 是使用SSL记录协议的三个特定协议之一(由SSL记录头格式的内容类型字段确定)，协议信息由单个字节消息组成；
- 虽然加密规范通常是在SSL握手协议结束时才被改变，但实际上，它可以在任何时候被改变。

SSL告警协议

- 告警是能够通过SSL记录协议进行传输的特定类型消息；
- 告警由两个部分组成：告警级别和告警说明，都用8比特进行编码；
- 告警有两个级别，第二个字节包含了特定警告代码，定义主要的告警类型；
- 告警消息也被压缩和加密。

SSL告警协议的告警类型

告警级别	告警名称	含　义
1	警告	表明一个一般告警信息
2	致命错误	致命错误，立即终止当前连接，同一会话的其它连接也许还能继续，但是肯定不会再产生新的连接

SSL告警协议的告警类型

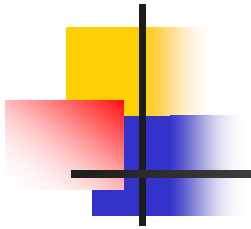
告警号	告警名称	含义
0	Close_notify	通知接收方发送方在本连接中不会再发送任何消息
10	Unexpected_message	接收到不适当的消息
20	Bad_record_mac	接收到的记录MAC错误(致命)
30	Decompression_failure	解压缩失败(致命)
40	Handshake_failure	发送方无法成功协调一组满意的安全参数设置(致命)
41	No_certificate	认证中心没有合适的证书
42	Bad_certificate	证书已经破坏

SSL告警协议的告警类型

告警号	告警名称	含义
43	Unsupported_certificate	不支持接收的证书类型
44	Certificate_revoked	证书已经撤销
45	Certificate_expired	证书过期
46	Certificate_unknown	在实现证书时产生了一些不确定问题
47	Illegal_parameter	握手过程某个字段超出范围或者与其它字段不符

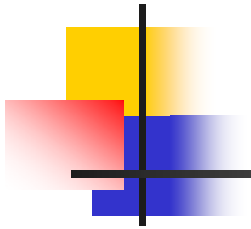
SSL协议的应用

- 主要用于支持HTTP服务，也可支持任何应用层协议，如Telnet、FTP等。
  - SSL可以作为具备安全能力的标准TCP/IP套接字API，因此，理论上SSL可以以安全的方式运行于任何TCP/IP应用程序之上，而不用对其做任何修改；
  - 大多数情况下，SSL仅被广泛用于HTTP连接，但也可用于其它应用程序类型，如网络新闻传输协议(NNTP)和Telnet。



网络层安全协议-----IPSec

- IPSec综述
- IPSec体系结构
- IPSec--- AH
- IPSec---ESP
- IPSec--IKE



IPSec综述

- 为了开发在网络层保护IP数据的方法，IETF成立了IP安全协议工作组(IPSec)，定义了一系列在IP层对数据进行加密的协议。
- IPSec（IP Security）是一种由IETF设计的端到端的确保IP层通信安全的机制。

IPSec综述

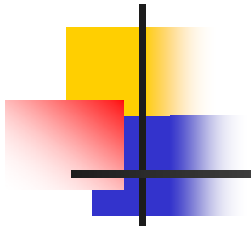
- IPSec的目的是要有效地保护IP数据包的安全。
  - 提供了一种标准的、强大的以及包容广泛的机制，为IP及上层协议提供安全保证；
  - 定义了一套默认的、强制实施的算法，以确保不同的实施方案相互之间可以共通，而且方便扩展；
  - 可保障主机之间、安全网关之间或主机与安全网关之间的数据包安全。
  - 由于受IPSec保护的数据包本身只是另一种形式的IP包，所以完全可以嵌套提供安全服务，同时在主机间提供端到端的验证，并通过一个安全通道，将那些受IPSec保护的数据传送出去。

IPSec综述

- IPSec不是一个单独的协议，而是一组协议。IPSec协议的定义文件包括了12个RFC文件和几十个Internet草案，已经成为工业标准的网络安全协议。
  - IP验证头(AH)协议
  - IP封装安全载荷协议(ESP)
  - Internet密钥交换协议（IKE）

IPSec综述

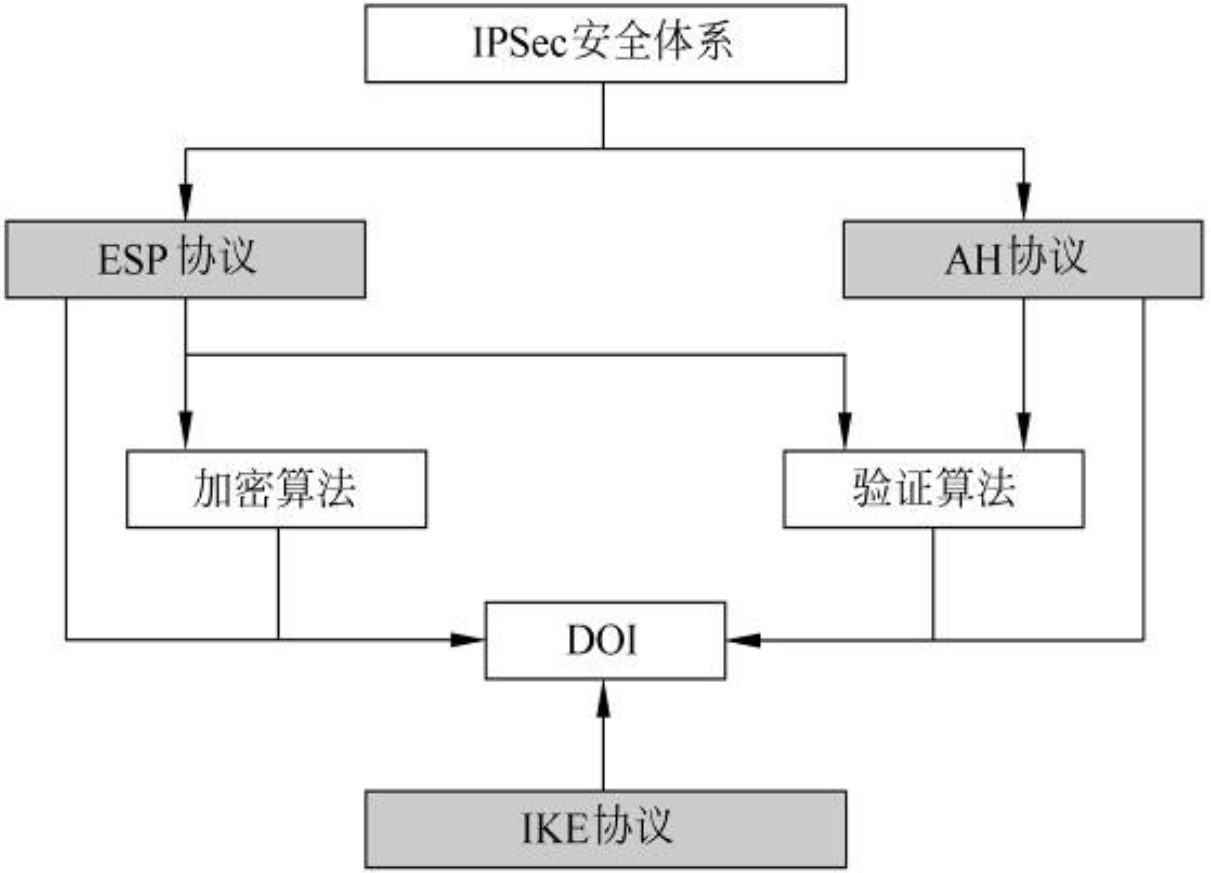
RFC	内容
2401	IPSec体系结构
2402	AH（Authentication Header）协议
2403	HMAC-MD5-96在AH和ESP中的应用
2404	HMAC-SHA-1-96在AH和ESP中的应用
2405	DES-CBC在ESP中的应用
2406	ESP（Encapsulating Security Payload）协议
2407	IPSec DOI
2408	ISAKMP协议
2409	IKE（Internet Key Exchange）协议
2410	NULL加密算法及在IPSec中的应用
2411	IPSec文档路线图
2412	OAKLEY协议



IPSec体系结构

- IPSec的协议簇体系
- IPSec保护数据的机理
- IPSec 的工作模式
- IPSec 的的数据包格式

IPSec的协议簇体系



IPSec保护数据的机理

- 认证：通过认证可以确定所接收的数据与所发送的数据是否一致，同时可以确定申请发送者在实际上是真实的还是伪装的发送者；
- 数据完整验证：通过验证，保证数据在从原发地到目的地的传送过程中没有发生任何无法检测的丢失与改变；
- 保密：使相应的接收者能获取发送的真正内容，而无关的接受者无法获知数据的真正内容。

IPSec 的工作模式

- IPSec有两种运行模式
  - 传输模式（Transport Mode）
  - 隧道模式（Tunnel Mode）。
- AH和ESP都支持这两种模式，因此有4种可能的组合：传输模式的AH、隧道模式的AH、传输模式的ESP和隧道模式的ESP。

IPSec的工作模式

- IPSec的传输模式
  - 传输模式要保护的内容是IP包的载荷，可能是TCP/UDP等传输层协议，也可能是ICMP协议。
  - 传输模式为上层协议提供安全保护，通常情况下，传输模式只用于两台主机之间的安全通信。
  - 正常情况下，传输层数据包在IP中被添加一个IP头部构成IP包。启用IPSec之后，IPSec会在传输层数据前面增加AH或者ESP或者二者同时增加，构成一个AH数据包或者ESP数据包，然后再添加IP头部组成新的IP包。

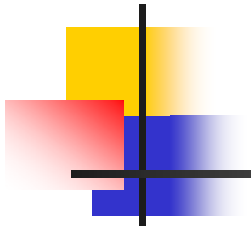
IPSec的工作模式

- IPSec的隧道模式
  - 隧道模式保护的内容是整个原始IP包，隧道模式为IP协议提供安全保护。通常情况下，只要IPSec双方有一方是安全网关或路由器，就必须使用隧道模式。
  - 如果路由器要为自己转发的数据包提供IPSec安全服务，就要使用隧道模式。路由器主要依靠检查IP头部来做出路由决定，不会也不应该修改IP头部以外的其他内容。如果路由器对要转发的包插入传送模式的AH或ESP头部，便违反了路由器的规则。

IPSec的工作模式

- IPSec的隧道模式
  - 路由器将需要进行IPSec保护的原始IP包看作一个整体，将这个IP包作为要保护的内容，前面添加AH或者ESP头部，然后再添加新的IP头部，组成新的IP包之后再转发出去。以ESP为例，示意如下。

应用ESP：IP+ESP[IP+TCP]



IPSec的工作模式

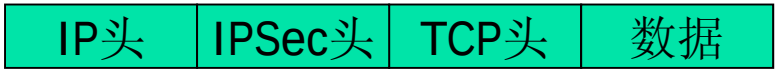
- IPSec的隧道模式
  - IPSec隧道模式的数据包有两个IP头：内部头和外部头。内部头由路由器背后的主机创建，外部头由提供IPSec的设备（可能是主机，也可能是路由器）创建。
  - 隧道模式下，通信终点由受保护的内部IP头指定，而IPSec终点则由外部IP头指定。如IPSec终点为安全网关，则该网关会还原出内部IP包，再转发到最终目的地。

IPSec的数据包格式

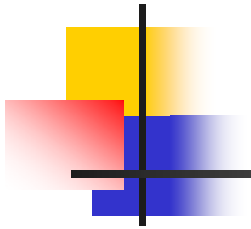
- 传送模式用来保护上层协议，而隧道模式用来保护整个IP数据报，以下是IPSec的数据包格式：

原始的IP包

传输模式下受保护的包



隧道模式下受保护的包



IPSec--- AH

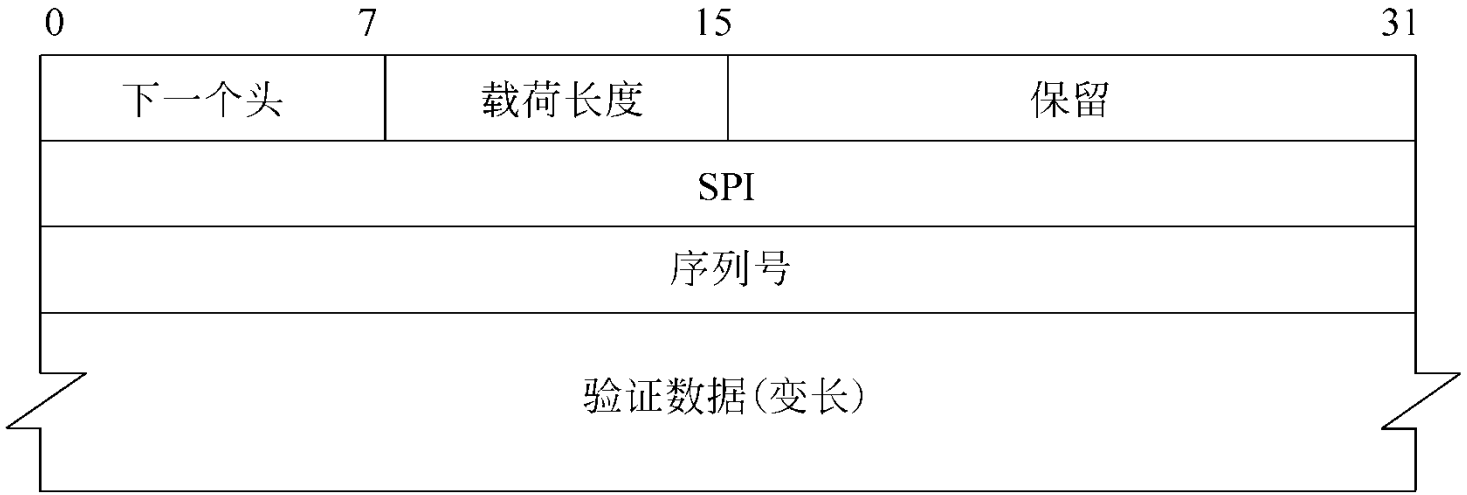
- AH（Authentication Header）
  - 称为验证头部协议，由RFC2402定义，是用于增强IP层安全的一个IPSec协议。
  - 该协议可以提供无连接的数据完整性、数据来源验证和抗重放攻击服务。

IPSec--- AH

- AH协议对IP层的数据使用密码学中的验证算法，从而使得对IP包的修改可以被检测出来。
  - MAC算法与HASH算法非常相似，区别在于MAC算法需要一个密钥（key），而HASH算法不需要。实际上，MAC算法一般是由HASH算法演变而来，也就是将输入报文和密钥结合在一起然后应用HASH算法。这种MAC算法称为HMAC，例如HMAC　MD5、HMAC　SHA1。
  - 通过HMAC算法可以检测出对IP包的任何修改，从而保证了IP包内容的完整性和IP包来源的可靠性。不同的IPSec系统，其可用的HMAC算法也可能不同，但是都必须支持HMAC-MD5和HMAC-SHA1。

AH的头部格式

- AH协议和TCP、UDP协议一样，是被IP协议封装的协议之一。一个IP包的载荷是否是AH协议，由IP协议头部中的协议字段判断，AH协议是51。
- 如果一个IP包封装的是AH协议，在IP包头（包括选项字段）后面紧跟的就是AH协议头部。



AH的头部格式

- 下一个头（Next Header）：最开始的8位，表示紧跟在AH头部的下一个载荷的类型，也就是紧跟在AH头部后面数据的协议。在传输模式下，该字段是处于保护中的传输层协议的值，比如6（TCP）、17（UDP）或者50（ESP）。在隧道模式下，AH所保护的是整个IP包，该值是4，表示IP-in-IP协议。
- 载荷长度（Payload Length）：接下来的8位，其值是以32位（4字节）为单位的整个AH数据（包括头部和变长的认证数据）的长度再减2。
- 保留（reserved）：16位，作为保留用，实现中应全部设置为0。

AH的头部格式

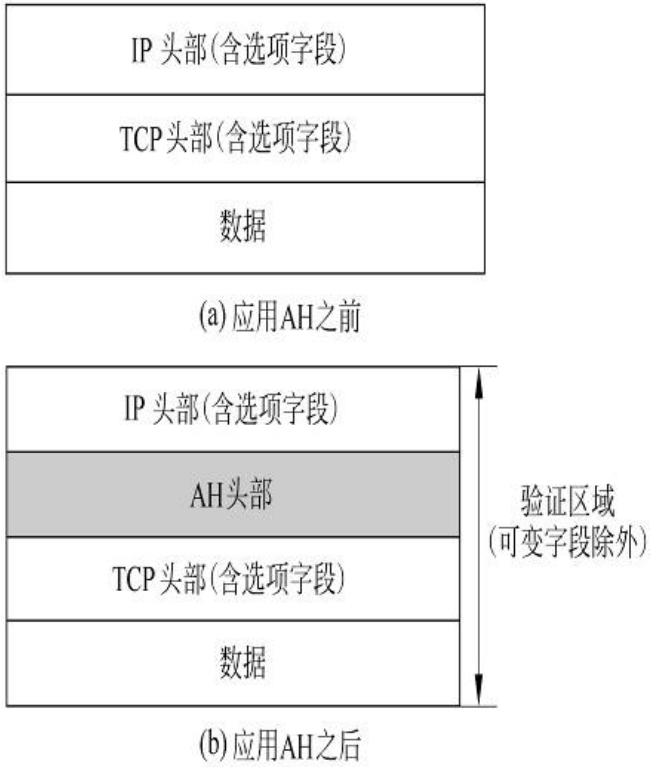
- SPI（Security Parameter Index，安全参数索引）：SPI是一个32位整数，与源/目的IP地址、IPSec协议一起组成的三元组可以为该IP包惟一地确定一个SA。[1，255]保留为将来使用，0保留本地的特定实现使用。因此，可用的SPI值为[256，232-1]。
- 序列号（Sequence Number）：序列号是一个32位整数，作为一个单调递增的计数器，为每个AH包赋予一个序号。当通信双方建立SA时，计数器初始化为0。SA是单向的，每发送一个包，外出SA的计数器增1；每接收一个包，进入SA的计数器增1。该字段可以用于抵抗重放攻击。
- 验证数据（Authentication Data）：可变长部分，包含了验证数据，也就是HMAC算法的结果，称为ICV（Integrity Check Value，完整性校验值）。该字段必须为32位的整数倍，如果ICV不是32位的整数倍，必须进行填充，用于生成ICV的算法由SA指定。

IPSec--- AH的运行模式

- AH包含两种运行模式：传输模式和隧道模式。
  - AH传输模式：AH插入到IP头部（包括IP选项字段）之后，传输层协议（如TCP、UDP）或者其他IPSec协议之前。
  - AH隧道模式：AH插入到原始IP头部字段之前，然后在AH之前再增加一个新的IP头部。隧道模式下，AH验证的范围也是整个IP包，因此AH和NAT的冲突在隧道模式下也存在。在隧道模式中，AH可以单独使用，也可以和ESP一起嵌套使用。

AH的传输模式

- 在传输模式中，AH插入到IP头部（包括IP选项字段）之后，传输层协议（如TCP、UDP）或者其他IPSec协议之前。
- 以TCP数据为例，右图表示了AH在传输模式中的位置。

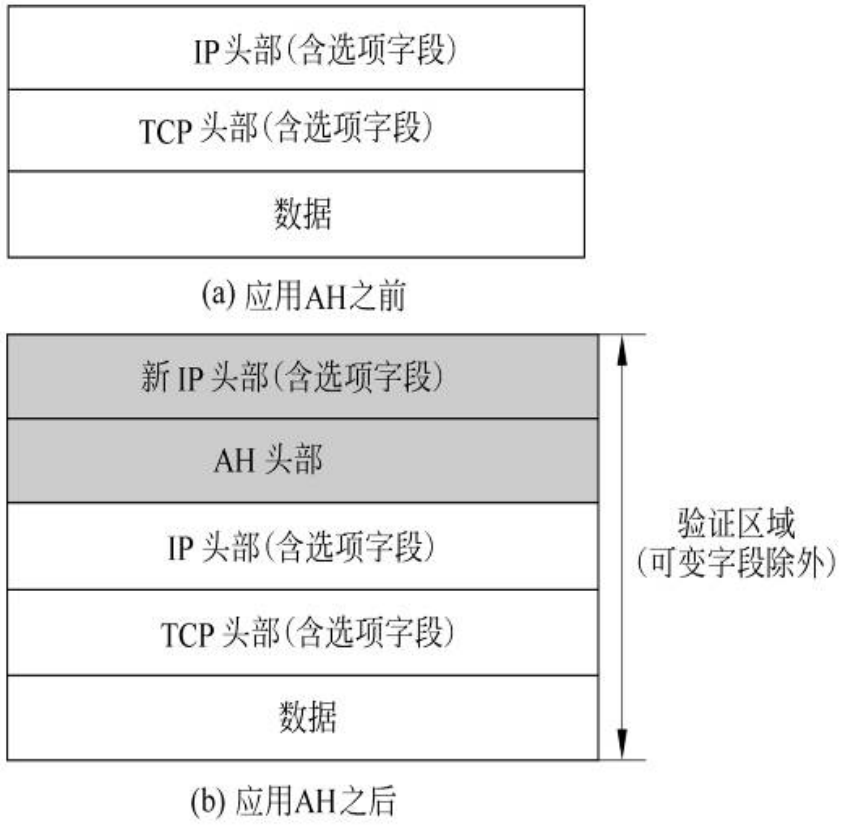


AH的传输模式

- 被AH验证的区域是整个IP包（可变字段除外），包括IP包头部，因此源IP地址、目的IP地址是不能修改的，否则会被检测出来。
- 如果该包在传送的过程中经过NAT网关，其源/目的IP地址将被改变，将造成到达目的地址后的完整性验证失败。因此，AH在传输模式下和NAT是冲突的，不能同时使用，或者可以说AH不能穿越NAT。

AH的隧道模式

- 在隧道模式中，AH插入到原始IP头部字段之前，然后在AH之前再增加一个新的IP头部。以TCP为例，右图表示了AH在隧道模式中的位置。



AH的数据完整性检查

- 在应用AH进行处理时，相应的SA应该已经建立，因此AH所用到的HMAC算法和密钥已经确定。
- AH协议验证的范围包括整个IP包，验证过程如下：
  - 在发送方，整个IP包和验证密钥被作为输入，经过HMAC算法计算后得到的结果被填充到AH头部的验证数据字段中；
  - 在接收方，整个IP包和验证算法所用的密钥也被作为输入，经过HMAC算法计算的结果和AH头部的验证数据字段进行比较，如果一致，说明该IP包数据没有被篡改，内容是真实可信的。

AH对IP报头字段的影响

- 在应用HMAC算法时，有一些因素需要考虑。在IP字段中，有一些是可变的，而且在传输过程中被修改也是合理的，不能说明该数据包是被非法篡改的。这些字段在计算HMAC时被临时用0填充。
  - ToS（Type of Service）：8位的服务类型字段指出了延时、吞吐量和可靠性方面的要求。
  - 表示分片的3位标志——DF（Don't Fragment）、MF（More Fragments）和0。路由器可能会修改这3个标志。
  - 分片偏移字段：标志字段后面的13位的偏移字段。
  - TTL：生命期，为了防止IP包的无限次路由，每经过一个路由器，该字段减1，当TTL变为0时，被路由器抛弃。
  - 头部校验和：中间路由器对IP包头部作了任何修改之后，必须重新计算头部校验和，因此该字段也是可变的。
  - 选项字段。
  - AH头部的验证数据字段在计算之前也要用0填充，计算之后再填充验证结果。

AH对IP报头字段的影响

- 对于一个IP包，除上述可变字段外，其余部分都认为是应该不变的，这些部分也正是受到AH协议保护的部分。
- 不变的部分包括：版本字段、头部长度字段、IP总长字段、ID字段、协议字段、源IP地址字段、目的地址字段、AH头中除验证数据以外的其他字段。
- 数据：指经过AH处理之后，在AH头部后面的数据。传输方式下，指TCP、UDP或ICMP等传输层数据；隧道模式下，指被封装的原IP包。

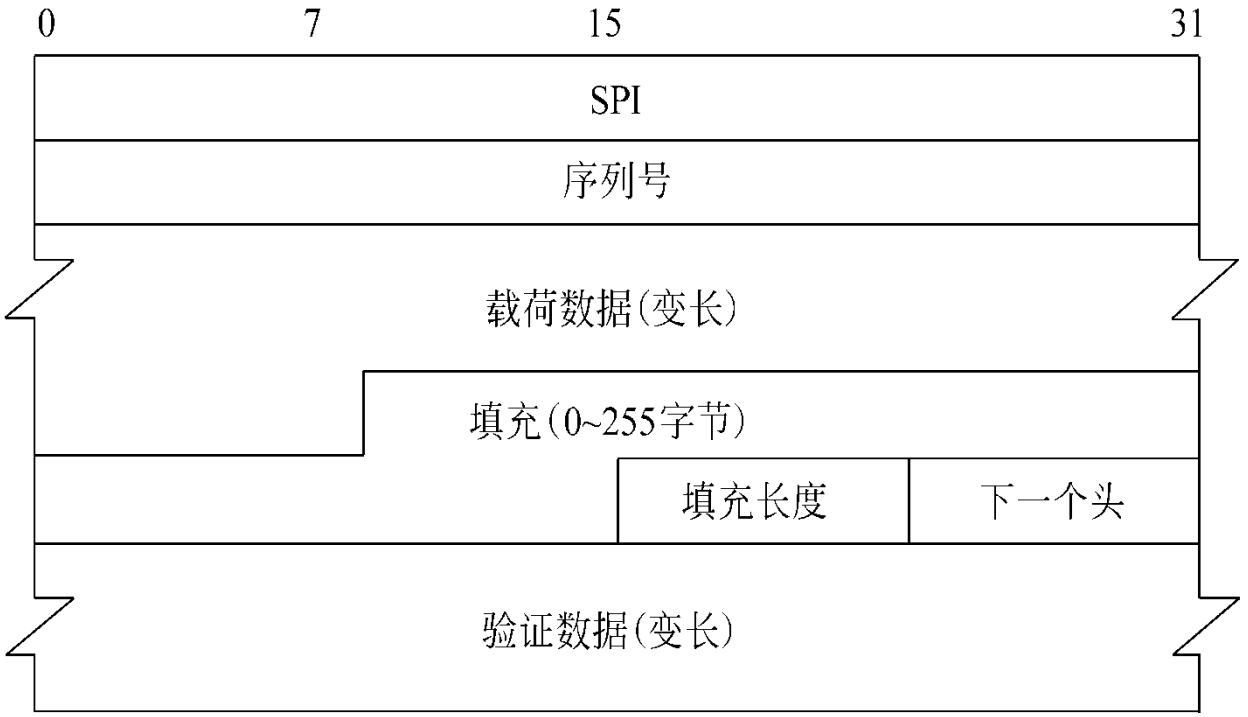
IPSec---ESP

- ESP(Encapsulating Security Payload)概述
  - ESP（封装安全载荷）协议也是一种增强IP层安全的IPSec协议，由RFC 2406定义。ESP协议除了可以提供无连接的完整性、数据来源验证和抗重放攻击服务之外，还提供数据包加密和数据流加密服务。
  - ESP协议提供数据完整性和数据来源验证的原理和AH一样，也是通过验证算法实现。数据包加密服务通过对单个IP包或IP包载荷应用加密算法实现；
  - ESP的加密采用的是对称密钥加密算法。不同的IPSec实现，其加密算法也有所不同。为了保证互操作性，ESP协议规定了所有IPSec系统都必须支持DES-CBC算法。

IPSec---ESP

- ESP协议和TCP、UDP、AH协议一样，是被IP协议封装的协议之一。
- 一个IP包的载荷是否是ESP协议，由IP协议头部中的协议字段判断，ESP协议字段是50。
- 如果一个IP包封装的是ESP协议，在IP包头（包括选项字段）后面紧跟的就是ESP协议头部。

ESP的头部格式



ESP的头部格式

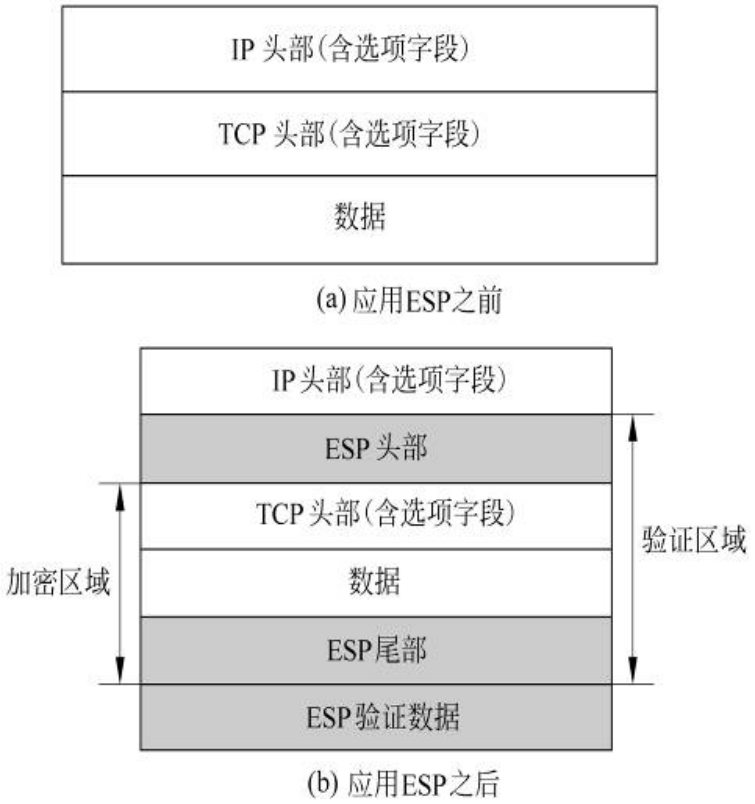
- SPI：SPI是一个32位整数，与源/目的IP地址、IPSec协议一起组成的三元组可以为该IP包惟一地确定一个SA。
- 序列号（Sequence Number）：序列号是一个32位整数，作为一个单调递增的计数器，为每个ESP包赋予一个序号。当通信双方建立SA时，计数器初始化为0。SA是单向的，每发送一个包，外出SA的计数器增1；每接收一个包，进入SA的计数器增1。该字段可以用于抵抗重放攻击。

ESP的头部格式

- 载荷数据（Payload Data）：这是必需的变长字段，包含了实际的载荷数据。如果采用了加密，该部分就是加密后的密文；如果没有加密，该部分就是明文。
- 填充（Padding）:填充字段包含了填充位。
- 填充长度（Pad Length）:填充长度字段是一个8位字段，以字节为单位指示了填充字段的长度，其范围为[0，255]。
- 下一个头（Next Header）:8位字段，指明了封装在载荷中的数据类型，例如6表示TCP数据。
- 验证数据（Authentication Data）。
- 变长字段：只有选择了验证服务时才会有该字段，包含了验证的结果。

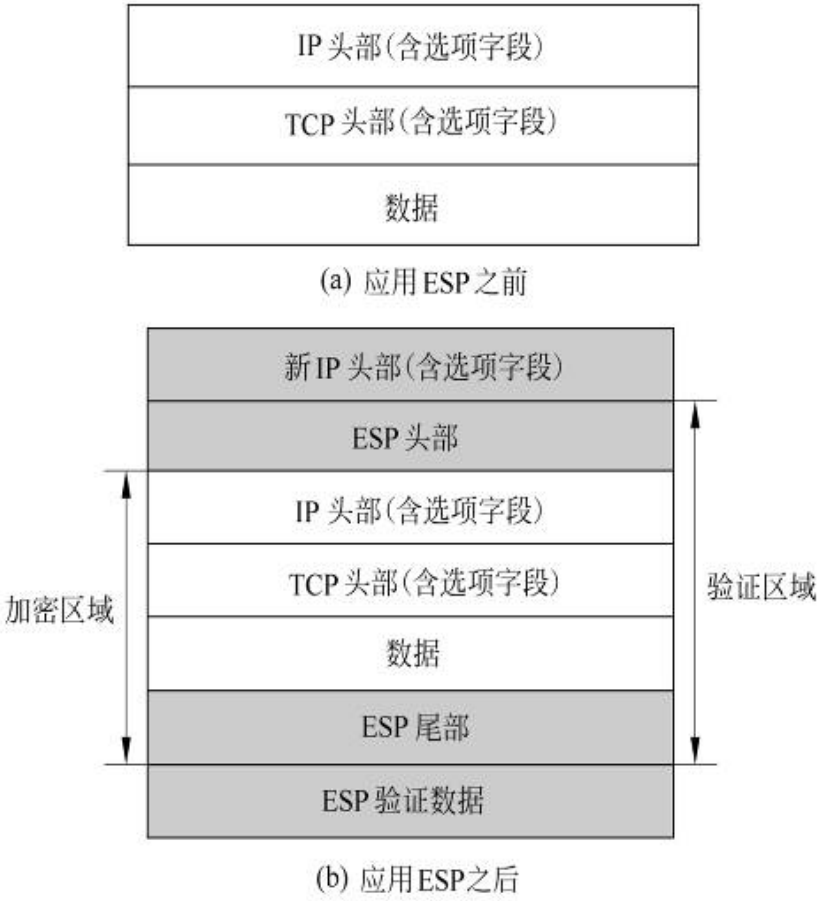
ESP的运行模式

- ESP的运行模式包括传输模式和隧道模式。
  - ESP传输模式:传输模式保护的是IP包的载荷，ESP插入到IP头部之后，任何被IP协议所封装的协议之前。



ESP的运行模式

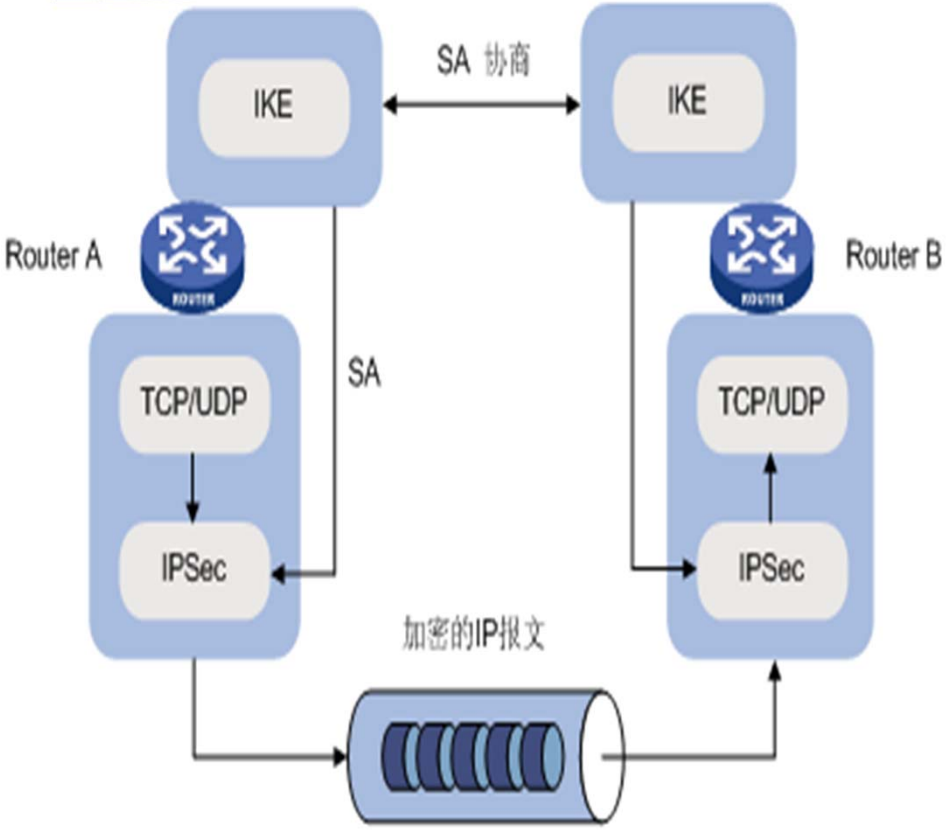
- ESP的运行模式包括传输模式和隧道模式。
  - 隧道模式保护的是整个IP包，对整个IP包进行加密。ESP插入到原IP头部（含选项字段）之前，在ESP之前再插入新的IP头部。



IPSec--IKE

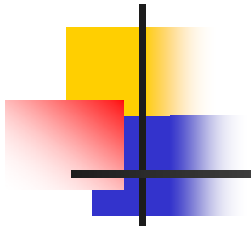
- IKE(Internet Key Exchange Protocol)在IPSec通信双方之间建立起共享安全参数及验证过的密钥。
- IKE通信可分以下几步进行：
  - 进行某种形式的协商；
  - Diffie-Hellman交换以及共享秘密的建立；
  - 对Diffie-Hellman共享秘密和IKE SA本身进行验证。
- IKE定义了五种验证方法：预共享密钥、数字签名(使用数字签名标准，即DSS)、数字签名(使用RSA公共密钥算法)、用RSA进行加密的nonce交换、用加密nonce进行的一种校订验证方法。其中，nonce是一种随机数字。

IPsec与IKE的关系



IPsec与IKE的关系

- IKE是UDP之上的一个应用层协议，是IPsec的信令协议；
- IKE为IPsec协商建立SA，并把建立的参数及生成的密钥交给IPsec；
- IPsec使用IKE建立的SA对IP报文加密或认证处理。



思考题

- TCP/IP体系下面临的安全威胁有哪些？
- 简述SSL协议保护数据的机理。
- 网络层的安全协议主要包括哪几个？
- 简述IPsec的功能。