

**网络安全**

适用班级：软件设计师 网络工程师

主讲：邓少勋

Q Q：154913686

网址：[www.bitpx.com](http://www.bitpx.com)

E-Mail:bitpx@163.com

分值说明：早上试题考5-10分

下午试题考15分(网工)

比特培训中心

贵州·贵阳

目 录

[第1节 网络安全基本概念 1](#_Toc526509710)

[1.1 网络安全的目标 1](#_Toc526509711)

[1.2 网络安全的脆弱性 1](#_Toc526509712)

[1.3 安全攻击的主要手段 1](#_Toc526509713)

[1.4 网络安全机制与技术 2](#_Toc526509714)

[1.5 历年试题 2](#_Toc526509715)

[第2节 信息加密技术 3](#_Toc526509716)

[2.1 数据加密原理 3](#_Toc526509717)

[2.2 经典加密技术 3](#_Toc526509718)

[2.3 现代加密技术 3](#_Toc526509719)

[2.3.1 对称密码体制 3](#_Toc526509720)

[2.3.2 非对称密码体制 4](#_Toc526509721)

[2.3.3 混合密码体制 5](#_Toc526509722)

[2.4 历年试题 5](#_Toc526509723)

[第3节 实体认证 6](#_Toc526509724)

[3.1 基于共享密钥的认证 6](#_Toc526509725)

[3.1.1 Needham-Schroeder认证协议 6](#_Toc526509726)

[3.2 基于公钥的认证 7](#_Toc526509727)

[3.3 历年试题 7](#_Toc526509728)

[第4节 数字签名 7](#_Toc526509729)

[4.1 基于共享密钥的数字签名 7](#_Toc526509730)

[4.2 基于公钥（非对称密钥）的数字签名 7](#_Toc526509731)

[4.3 历年试题 8](#_Toc526509732)

[第5节 数字证书 8](#_Toc526509733)

[5.1 数字证书 8](#_Toc526509734)

[5.2 认证中心CA 9](#_Toc526509735)

[5.3 历年试题 9](#_Toc526509736)

[第6节 密钥管理 10](#_Toc526509737)

[6.2 KMI技术 10](#_Toc526509738)

[6.3 PKI技术 10](#_Toc526509739)

[6.4 历年试题 10](#_Toc526509740)

[第7节 消息摘要 10](#_Toc526509741)

[7.1 常用的消息摘要算法 10](#_Toc526509742)

[7.2 历年试题 10](#_Toc526509743)

[第8节 无线局域网安全协议 11](#_Toc526509744)

[8.1 WLAN安全协议 11](#_Toc526509745)

[8.2 历年试题 11](#_Toc526509746)

[第9节 虚拟专用网VPN 12](#_Toc526509747)

[9.1 第二层隧道协议 12](#_Toc526509748)

[9.2 第三层IPSec隧道协议 13](#_Toc526509749)

[9.2.1 IPSec作用 13](#_Toc526509750)

[9.2.2 安全关联SA 13](#_Toc526509751)

[9.2.3 认证头AH 13](#_Toc526509752)

[9.2.4 封装安全负载ESP 14](#_Toc526509753)

[9.2.5 带认证的封装安全负载(ESP) 14](#_Toc526509754)

[9.2.6 Internet密钥交换协议IKE 15](#_Toc526509755)

[9.3 高层隧道协议 15](#_Toc526509756)

[9.3.1 SSL/TLS协议 15](#_Toc526509757)

[9.3.2 SOCKS协议 15](#_Toc526509758)

[9.4 历年试题 15](#_Toc526509759)

[第10节 应用层安全协议 16](#_Toc526509760)

[10.1 SSH（Secure Shell）协议 16](#_Toc526509761)

[10.2 S-HTTP 16](#_Toc526509762)

[10.3 PGP（Pretty Good Privacy）协议 16](#_Toc526509763)

[10.4 S/MIME 16](#_Toc526509764)

[10.5 安全的电子交易 16](#_Toc526509765)

[10.6 Kerberos服务 17](#_Toc526509766)

[10.7 RADIUS协议 17](#_Toc526509767)

[10.7.1 RADIUS的基本描述 17](#_Toc526509768)

[10.7.2 RADIUS的工作原理 18](#_Toc526509769)

[10.8 IEEE802.1x协议 18](#_Toc526509770)

[10.9 历年试题 18](#_Toc526509771)

[第11节 网络体系结构 20](#_Toc526509772)

[11.2 历年试题 20](#_Toc526509773)

[第12节 防火墙 21](#_Toc526509774)

[12.1 防火墙的基本类型 21](#_Toc526509775)

[12.1.1 包过滤防火墙 21](#_Toc526509776)

[12.1.2 状态检测防火墙 21](#_Toc526509777)

[12.1.3 应用代理防火墙 21](#_Toc526509778)

[12.2 典型防火墙拓扑结构 21](#_Toc526509779)

[12.3 历年试题 22](#_Toc526509780)

[第13节 病毒防护 23](#_Toc526509781)

[13.1 病毒的类型 23](#_Toc526509782)

[13.2 常见的病毒及木马、蠕虫等 23](#_Toc526509783)

[13.3 历年试题 23](#_Toc526509784)

[第14节 入侵检测系统 24](#_Toc526509785)

[14.1 IDS的入侵检测分析方法 24](#_Toc526509786)

[14.2 入侵检测系统的部署 24](#_Toc526509787)

[14.3 历年试题部分 25](#_Toc526509788)

[第15节 入侵防御系统 26](#_Toc526509789)

[15.1 入侵防御系统与防火墙及IDS区别 26](#_Toc526509790)

[15.2 IPS部署方式 26](#_Toc526509791)

# 网络安全基本概念

## 网络安全的目标

#### 可靠性：网络系统能在规定的时间内和规定的条件下完成规定的功能。

#### 可用性：网络信息系统可被授权实体访问并按需求使用的特性。

#### 真实性：确保网络信息系统的访问者与其声称的身份是一致的；确保网络应用程序的身份和功能与其声称的身份和功能是一致的；确定网络信息系统操作的数据是真实有效的数据。

#### 保密性：防止信息泄露给非授权的个人或实体，只允许授权用户访问的特性。保密性是一种面向信息的安全性，它建立在可靠性和可用性的基础之上，是保障网络信息系统安全的基本要求。

#### 完整性：信息在未经授权时不能被改变的特性，即信息生成、信息储存或传输过程中保证不被偶然或蓄意地删除、修改、伪造、乱序、插入等破坏和丢失的特性。

#### 不可抵赖性：也称为不可否认性，即在网络信息系统的信息交互过程中所有参与者都不可能否认或抵赖曾经完成的操作的特性。

## 网络安全的脆弱性

#### 体系结构的脆弱性：网络体系结构要求上层调用下层的服务，上层是服务的调用者，下层是服务器的提供者，当下层提供的服务出错时，会使上层的工作受到影响。

#### 网络通信的脆弱性：网络安全通信是实现网络设备之间、网络设备与主机节点之间进行信息交换的保障，然而通信协议或通信系统的安全缺陷往往危及到网络系统的整体安全。

#### 网络操作系统的脆弱性：Windows、UNIX、Netware等网络操作系统都不断爆出各种漏洞，这些漏洞被攻击者发现会威胁到整个网络的安全。

#### 网络应用系统的脆弱性：和网络操作系统的脆弱性一样，网络应用系统的脆弱性也会被攻击者利用，从而威胁到网络的安全。

#### 网络管理的脆弱性：网络管理工作当中的安全意识淡薄、安全制度不健全、岗位职责混乱、审计不力、设备选型不当和人事管理漏洞等都会带来网络的巨大安全问题。

## 安全攻击的主要手段

网络威胁是对网络安全缺陷的嵌在利用，这些缺陷可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏等。

#### **窃听**：在广播式的网络系统中，每个节点都可以读取网上传输的数据，如搭线窃听、安装通信监视器和读取网上的信息等。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目标地址，这种特性使得偷听网上的数据或非授权访问很容易而且不易发现。如常见的sniffer攻击，就是一种窃听方式。

#### **数据篡改（数据完整性破坏）**：网络攻击者通过未授权的方式，非法读取并篡改数据，以达到通信用户无法获取真实信息的攻击目的。

#### **盗用口令攻击（password-based attacks）**：攻击者通过多种途径获得合法用户的账号和密码后进入目标网络，从而进行破坏性的活动。

#### **中间人攻击(man-in-the-middle attack)**：通过第三方进行网络攻击，以达到欺骗被攻击系统、反跟踪、包含攻击或者组织大量规模攻击的目的。中间人攻击类似于身份欺骗，被利用作为中间人的主机称为Remote Host（黑客取其谐音为“肉鸡”）。网络上大量计算机被黑客通过这样的方式控制，这样的主机称为僵尸主机。

#### **缓冲区溢出**：攻击者输入的数据长度超过应用程序给定的缓冲区的长度，覆盖其他数据区，造成应用程序错误，而覆盖缓冲区的数据恰恰是黑客的入侵程序代码，黑客就可以获取程序的控制权，以达到攻击目的。

#### **假冒**：一个实体假扮成另外一个实体进行网络活动。如地址欺骗、电子邮件欺骗、Web欺骗和非技术类欺骗、网络钓鱼等手段。

#### **重放**：重复一份报文或报文的一部分，以便产生一个被授权的效果。

#### **流量分析**：由于数据报头信息不能加密，所以即使加密也只能对数据部分进行加密，故攻击者可通过对网上信息流的观察和分析推断出网上传输信息中的有用信息。

#### **拒绝服务(DoS:Denial of Service)**：通常是使用极大的通信量冲击网络系统，使得所有的可用网络资源都被消耗殆尽，最后导致网络系统无法向合法的用户提供服务。如果攻击者组织多个攻击点对一个或多个目标同时发动DoS攻击，就可以极大地提高DoS攻击的威力，这种方式称为DDoS（Distributed Denial of Service，分布式拒绝服务）攻击。

#### **分发攻击**：在系统的软硬件生产或分发期间对其软件或硬件进行恶意修改或破坏，以其感染系统的正常运行，或者事后能对信息系统进行非授权访问及破坏，或者利用系统或管理人员向用户分发账号和密码的过程窃取资料。

#### **野蛮攻击**：包括字典攻击和穷极攻击。

#### **SQL注入攻击**：利用对方的SQL数据库和网站的SQL语句漏洞来进行攻击。入侵者通过提交一段数据库查询代码，根据程序返回的结果获得攻击者想要的数据或者提高访问的权限，从而达到攻击目的。

#### **ARP欺骗**：ARP在进行地址解析的工作工程中，没有对数据报和发送实体进行真实性和有效性的验证，因此存在安全缺陷。攻击者可以通过发送伪造的ARP消息给攻击对象，使被攻击对象获得错误的ARP解析。例如，攻击者可以伪造网关的ARP解析，使被攻击对象将发给网关的数据报错误地发送到攻击者所在主机，于是攻击者就可以窃取、篡改、阻断数据的正常转发，一直造成整个网段的瘫痪。

#### XSS和CSRF攻击。XSS又称CSS（Cross Site Script，跨站点脚本），攻击者在Web页面或url上加入恶意脚本，当其他用户访问和执行脚本时，就可以获取用户的敏感数据，达到攻击目的。CSRF（Cross Site Request Script，跨站点请求伪造）的攻击者伪造恶意脚本，使得浏览者在未知情况下执行Web请求，导致数据被篡改或者蠕虫的传播。

#### **资源的非授权访问**：对资源的使用不在指定的安全策略范围内。

#### **陷门(backdoor attack)：**又称为后门，指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么它就成了安全风险，容易被黑客当成漏洞进行攻击。

#### **特洛伊木马**：简称木马，伪装成正常的软件程序进入用户的计算机，在感染用户计算机后窃取用户资料如QQ账号和密码、网银账号和密码等用户敏感信息传递给攻击者，或者使攻击者可以控制用户计算机。木马由两部分组成：**控制端和服务端(C/S模式)**。被感染的用户计算机上嵌入的是服务端，而攻击者方为控制端。木马一般不破坏用户计算机的数据，主要是盗取数据。

#### **病毒**：一段可执行程序，通过对其他程序进行修改，可以感染这些程序使其含有该病毒的一个拷贝。病毒可以做其他程序所做的任何事情，唯一的区别在于它将自己附在另外一个程序上，并且在宿主程序运行时秘密执行。一旦病毒执行时，它可能会进行修改、删除等破坏用户数据的行为，也可能导致用户计算机的软、硬件正常运行受到很严重的影响。

#### **诽谤**：利用计算机信息系统的广泛互联性和匿名性，散步错误的消息以达到诋毁某个对象的形象和知名度的目的。

#### **蠕虫(worm)** ：是一种智能化、自动化、综合网络攻击、密码学和计算机病毒的技术。病毒是通过修改其他程序而将其感染，而蠕虫是独立的一种智能程序，它可通过网络等途径将自身的全部代码或部分代码复制、传播给其他的计算机系统，蠕虫不寄生于宿主程序。同时具备病毒和蠕虫特点的程序称为蠕虫病毒，具备极强的破坏能力。

在开放式网络中，网络通信会遭受两种方式的攻击：**主动攻击和被动攻击。主动攻击包括对用户信息的篡改、删除及伪造，对用户身份的冒充和对合法用户访问的阻止。被动攻击包括对用户信息的窃取、对数据流量的分析等。**

## 网络安全机制与技术

#### **数据加密**：目前网络中采用的最基本的安全技术。加密技术提高了信息系统及数据的安全性和保密性，是防止密码数据被外部窃取所采用的主要技术之一；

#### **数字签名**：用来证明消息确实由发送者签发的，而且，当数字签名用于存储的数据或程序时，可以用来验证数据或程序的完整性；

#### **身份认证**：有多种方法用来认证一个用户的合法性，如密码技术、利用人体生理特征(如指纹)进行识别、智能IC卡和USB盘等；

#### **防火墙**：一种通信过滤技术，通过控制和检测网络之间的信息交换和访问行为来实现对网络安全的有效管理；

#### **入侵检测**：是对防火墙的合理补充，以帮助系统对付网络攻击。IDS(Intrusion Detection System，入侵检测系统)收集和分析网络或主机系统的通信情况，检查是否存在违反安全策略和遭到袭击的迹象；

#### **内容检查**：查毒软件一般对数据内容和程序构成进行内容检查，看是否感染病毒。

## 历年试题

●(2005年下)窃取是对 (31) 的攻击，DDos攻击破坏了(32)。

（31）A. 可用性　　B. 保密性　　C. 完整性　　D. 真实性

（32）A. 可用性　　B. 保密性　 C. 完整性　　D. 真实性

●(2006年上)驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于 (39) 。

(39)A. 上网冲浪　　　B. 中间人攻击　　　 C. DDoS 攻击　 　D. MAC攻击

●(2006年下)许多黑客利用软件实现中的缓冲区溢出漏洞进行攻击，对于这一威胁，最可靠的解决方案是（33）。

（33）A. 安装防火墙 B. 安装用户认证系统 C. 安装相关的系统补丁软件 D. 安装防病毒软件

●(2006年下)（34）无法有效防御 DDoS 攻击。

（34）A. 根据 IP 地址对数据包进行过滤B. 为系统访问提供更高级别的身份认证

C. 安装防病毒软件 D. 使用工具软件检测不正常的高流量

●[2007年上]下列行为不属于网络攻击的是 （7） 。

（7）A.连续不停ping某台主机 B.发送带病毒和木马的电子邮件C.向多个邮箱群发一封电子邮件 D.暴力破解服务器密码

●(2007年上)多形病毒指的是（47）的计算机病毒。

（47）A.可在反病毒监测时隐藏自己B.每次感染都会改变自己C.可以通过不同的渠道进行传播D.可以根据不同环境造成不同破坏

●(2008年下)为了防止电子邮件中的恶意代码，应该用 （39） 方式阅读电子邮件。

（39）A.纯文本 B.网页 C.程序 D.会话

●(2008年下)“TCP SYN Flooding”建立大量处于半连接状态的TCP连接，其攻击目标是网络 （43） 。

（43）A.保密性 B.完整性 C.真实性 D.可用性

●(2008年下)计算机感染特洛伊木马后的典型现象是（45）。

（45）A.程序异常退出 B.有未知程序试图建立网络连接 C.邮箱被邮件垃圾填满 D.Windows系统黑屏

●(2009年上)下面通过ARP木马的描述中，错误的是（49）。

（49）A．ARP木马利用ARP协议漏洞实现破坏 B. ARP木马发作可导致网络不稳定甚至瘫痪

C. ARP木马破坏网络的物理连接 D. ARP木马把虚假的网关MAC地址发送给受害主机

●(2009年上)网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（68）。

（68）A．多重安全网关 B.防火墙 C．VLAN隔离 D.物理隔离

●(2010年下)如果使用大量的连接请求攻击计算机，使得所有可用的系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求，这种手段属于 （7）攻击。

（7）A.拒绝服务 B.口令入侵 C.网络监听 D.IP欺骗

●(2010年下)ARP攻击造成网络无法跨网段通信的原因是(8)。

（8）A.发送大量ARP报文造成网络拥塞 B.伪造网关ARP报文使得数据包无法发送到网关

C.ARP攻击破坏了网络的物理的连通性D.ARP攻击破坏了网关设备

●(2012年上)以下关于钓鱼网站的说法中，错误的是（42）。

(42)A．钓鱼网站仿冒真实网站的URL地址 B．钓鱼网站是一种网络游戏

C．钓鱼网站用于窃取访问者的机密信息 D．钓鱼网站可以通过Email传播网址

●(2012年上)网络的可用性是指（46）。

(46)A．网络通信能力的大小 B．用户用于网络维修的时间 C．网络的可靠性 D．用户可利用网络时间的百分比

●(2013年下)下列网络攻击行为中，属于DoS攻击的是（41） 。

（42）A.特洛伊木马攻击 B.SYN Flooding攻击 C.端口欺骗攻击 D.IP欺骗攻击

●(2014年上)以下关于木马程序的叙述中，正确的是 (7) 。

(07)A．木马程序主要通过移动磁盘传播 B．木马程序的客户端运行在攻击者的机器上

C．木马程序的目的是使计算机或网络无法提供正常的服务 D．Sniffer是典型的木马程序

●(2014年下)以下关于拒绝服务攻击的叙述中，不正确的是 (8) 。

(8)A.拒绝服务攻击的目的是使计算机或者网络无法提供正常的服务

B.拒绝服务攻击是不断向计算机发起请求来实现的

C.拒绝服务攻击会造成用户密码的泄漏

D.DDoS是一种拒绝服务攻击形式

●(2015年上) (66) 针对TCP连接进行攻击。

(66)A.拒绝服务 B.暴力攻击 C.网络侦察 D.特洛伊木马

●(2015年上)安全需求可划分为物理安全、网络安全、系统安全和应用安全，下面的安全需求中属于系统安全的是 (67) ，属于应用安全的是 (68) 。

(67)A.机房安全 B.入侵检测 C.漏洞补丁管理 D.数据库安全

(68)A.机房安全 B.入侵检测 C.漏洞补丁管理 D.数据库安全

●(2015年下) (41)不属于主动攻击。

（41）A.流量分析 B.重放 C.IP地址欺骗 D.拒绝服务

●(2016年下)在网络设计和实施过程中要采取多种安全措施，下面的选项中属于系统安全需求措施的是 (68) 。

(68)A.设备防雷击 B.入侵检测 C.漏洞发现与补丁管理 D.流量控制

●(2017年下)下列攻击行为中属于典型被动攻击的是 (42) 。

(42)A.拒绝服务攻击 B.会话拦截 C.系统干涉 D.修改数据命令

●(2018年上)攻击者通过发送一个目的主机已经接收过的报文来达到攻击目的，这种攻击方式属于（42）攻击。

（42）A.重放 B.拒绝服务 C.数据截获 D.数据流分析

# 信息加密技术

在网络传输过程中，信息存在被非法窃听的危险，因此对信息进行加密是网络安全的基本技术。

## 数据加密原理

研究数据加密的科学叫做密码学（Cryptography），它又分为**设计密码体制的密码编码学和破译密码的密码分析学**。

一般的保密通信模型如图 2.1所示。在发送端，把明文P用加密算法E和密钥K加密，变换成密文C，即，在接收端利用解密算法D和密钥K对密文C进行解密得到明文P，即，**加解密算法E和D是公开的，而密钥K（加解密函数的参数）是保密的。**在传送过程中，偷听者得到的是无法理解的密文，由于他没有密钥，所以不能对数据解密，这就实现对第三者保密的目的。

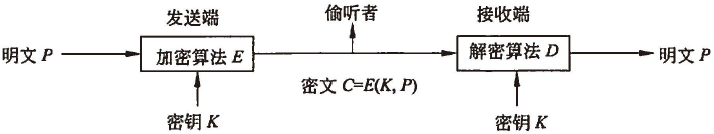


图 2.1保密通信模型

## 经典加密技术

主要有三种经典的加密技术：替换加密（substitute）、换位加密（transposition）、一次性填充（one-time pad）。

## 现代加密技术

现代密码体制使用的基本方法仍然是替换和换位，但采用更加复杂的加密算法和简单的密钥。而且增加了对付主动攻击的手段，例如**加入随机的冗余信息防止制造假信息；加入时间控制信息，防止旧消息重放攻击。**

现代密码体制可以分为两类：**对称密码体制和非对称密码体制，还有前两者相结合的混合密码体制。**

### 对称密码体制

对称密码体制也称**会话密钥加密算法、单密钥体制、共享密码算法或私钥密码体制**，其特点是加密和解密所用的密钥是一样的或相互可以导出。

**常用对称密钥体制的加密算法有：DES算法，3DES算法，TDEA算法，Blowfish算法，RC算法，IDEA算法和AES算法等**。

如图 2.2所示，对称密钥体制可看成保险柜，密钥就是保险柜的号码。持有号码的人就能打开保险柜取出文件，没有保险柜号码的人就必须摸索保险柜的打开方法。当用户应用这种体制时，数据的发送者和接收者必须事先通过安全渠道交换密钥，以保证发送数据和接收数据能够使用有效的密钥。

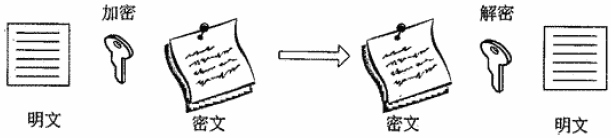


图 2.2对称密钥体制的加解密流程

**对称密钥体制的优点是加密数据效率高、速度快，故对称密钥非常适合于大量数据加密或实时加密（如文件加密或实时数据加密）。**

联邦数据加密DES（Data Encryption Standard）算法

DES算法，它使**用56位密钥**对**64位**的数据块进行加密，并对64位的数据进行**16轮编码**，在每轮编码时都采用不同的子密钥，子密钥长度均为48位，由56位的完整密钥得出，最终得到**64位的密文,如**图 2.3**所示**。由于DES算法密钥较短，可以通过穷举（也称为野蛮攻击）的方法在较短时间内破解。

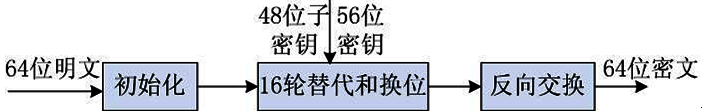


图 2.3 DES加密过程

三重DES（Triple-DES）

这种方法是DES的改进算法，它使用**两把密钥对报文作三次DES加密**，效果相当于将DES密钥长度加倍了，克服了DES密钥长度较短的缺点。

假设两个密钥分别是K1和K2，其算法的步骤如下，如图 2.4所示：

##### 用密钥K1进行DES加密；

##### 用K2对步骤（1）的结果进行DES解密；

##### 对步骤（2）的结果使用密钥K1进行DES加密。

**这种方法的缺点是要花费原来三倍的时间，但密钥长度加长，为112位（56\*2=112），更安全了。**



图 2.4 3DES加密过程

欧洲加密算法IDEA（International Data Encryption Algorithm,国际数据加密算法）

**密钥长度为128位，数据块长度为64位，IDEA算法也是一种数据块加密算法**，它设计了一系列的加密轮次，每轮加密都使用从完整的加密密钥生成一个子密钥。**IDEA属于强加密算法，至今还没有出现对IDEA进行有效攻击的算法。**

高级加密标准（Advanced Encryption Standard,AES）

**AES支持128,192和256位三种密钥长度。**AES规定：**块长度必须是128位，密钥长度必须是128,192位或者256位。**与DES一样，它也使用替换和换位操作，并且也使用多轮迭代的策略，具体的迭代轮数取决于密钥的长度和块的长度。该算法的设计提高了安全性，也提高了速度。

RC（Rivest Cipher）序列算法

RC算法目前有6个版本，其中RC1从未被公开，RC3在设计过程中便被破解，因此真正得到实际应用的只有RC2、RC4、RC5和RC6，其中最常用的是RC4。

* RC4

**RC4算法是另一种变长密钥的流加密算法。密钥长度介于1～2048位之间**，但由于美国出口限制，故向外出口时密钥长度一般为40位。

RC4算法其实非常简单，就是256内的加法，置换和异或运算。**由于简单，所以速度快，加密的速度可达到DES算法的10倍。**

总的特点：**加密速度快，适合加密大容量数据和实时加密。**

### 非对称密码体制

**非对称加密体制又称公钥密码体制：创建两个密钥，一个作为公钥，另外一个作为私钥。私钥由密钥拥有人个人保管，公钥和加密算法可以公开。用公钥加密的数据只有私钥才能解开，同样，用私钥加密的数据也只能用公钥才能解开。**

具体而言，每一个用户A有一个加密密钥和解密密钥。作为公钥可以公开，作为私钥必须个人保密存储。每一个要与A通信的用户B，只要获得A的公钥，便可用将明文P加密成密文C，即，B把密文C送给A之后，A用只有自己才掌握的私钥对C进行解密得到明文P，即，任何第三方即使截获密文C，或拿到公钥，都无法从与C中推导出，也就无法恢复明文P。

如图 2.5所示，公钥密码体制可看作邮箱，任何人都容易把邮件放进邮箱，只要知道地址进行投递就可以了。把邮件放进邮箱是一件公开的事情，但是打开邮箱却需要持有秘密信息（私钥或组合密码）才能进行。

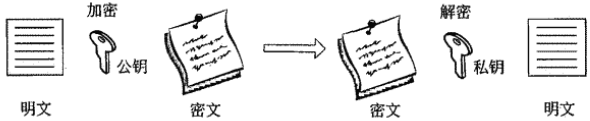


图 2.5非对称密码体制的加解密流程

与对称密码体制相比，公钥密码体制有以下优点：

* 密钥分发方便。可以用公开方式分配加密密钥。例如，因特网中的个人安全通信常将自己的公钥公布在网页中，方便其他人用它进行安全加密。
* 密钥保管量少。网络中的数据发送方可以共享一个公开加密密钥，从而减少密钥数量。只要接收方的解密密钥保密，数据的安全性就能实现。
* 支持数字签名。发送方可使用自己的私钥加密数据，接收方能用发送方的公钥解密，说明数据确实是发送方发送的。

**由于非对称加密算法处理大量数据的耗时较长，一般不适于大文件的加密，更不适于实时的数据流加密。**

Diffie-Hellman算法

Diffie-Hellman（DH）算法是第一个公钥算法，其安全性基于**计算离散对数的难度**，已在很多商业产品中得以应用。**此算法只能使用户安全地交换会话密钥（共享密钥），本身不能用于数据加、解密。**

RSA（Rivest Shamir and Adleman）算法

一种公钥加密算法，按照下面的要求选择公钥和密钥。

##### 选择**两个大素数**p和q(大于10100)；

##### 令n=p\*q和z=(p-1)\*(q-1);

##### 选择d与z互质；

##### 选择e，使e\*d=1（mod z）。

明文P被分成k位的块，k是满足2k<n的最大整数，于是有O≤P<n。加密时计算，这样**公钥**为**(e,n)**，解密时计算，即**私密**为**(d，n)**。

**RSA的优点是不需要密钥分配，但缺点是速度慢。**

●(2010年下半年)按照 RSA算法，若选两奇数p=5，q=3，公钥e＝7，则私钥d为（41）。

（41）A.6 **B. 7** C. 8 D. 9

补充：RSA、DSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）都是属于非对称加密算法。

### 混合密码体制

* 利用公钥密码体制分配对称密码体制的密钥;
* 数据的收发双方共享这个密钥，然后按照对称密码体制方式进行加密和解密运算。

混合密码体制的工作原理如图 2.6所示。第1步，消息发送者A产生**一个随机数**作为对称密钥，用对称密钥把需要发送的消息进行加密。第2步，A用B的公开密钥将对称密钥加密形成**数字信封**，然后把被加密的消息和数字信封一起传给B。第3步，B收到A的被加密的消息和数字信封后，用自己的私钥将数字信封解密，获取A加密数据时所用的对称密钥。第4步，B使用A加密的对称密钥把收到的被加密消息解开，从而得到明文。

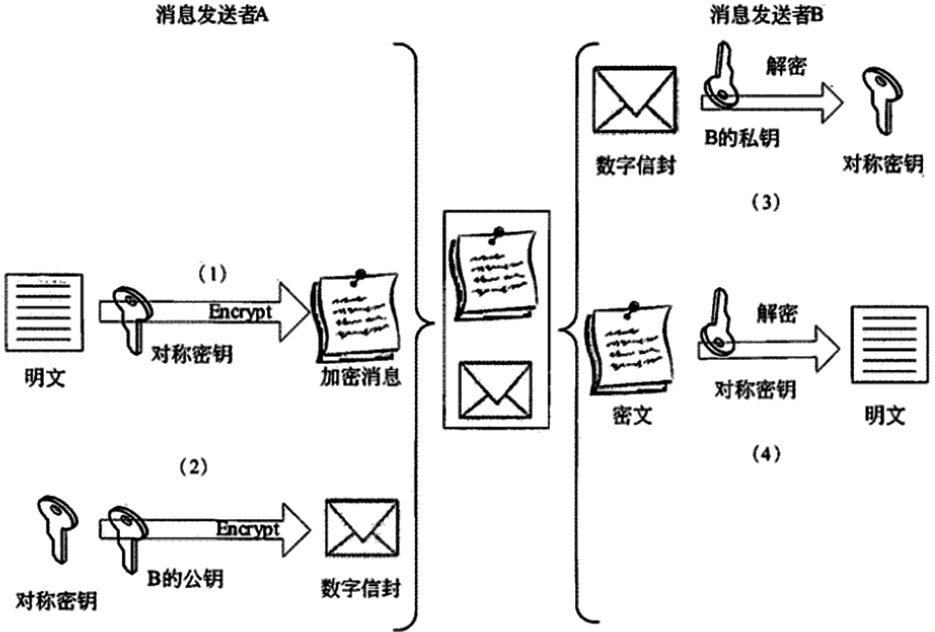


图 2.6混合密码体制的加密和解密流程

## 历年试题

●(2005年下)数据加密标准（DES）是一种分组密码，将明文分成大小 (33) 位的块进行加密，密钥长度为 (34) 位。

（33）A. 16　　B. 32　 C. 56　 D. 64 （34）A. 16　　B. 32　 C. 56 　D. 64

●(2007年上)DES是一种（40）算法

（40） A.共享密钥 B.公开密钥 C.报文摘要 D.访问控制

●(2008年下)常用对称加密算法不包括 （41） 。

（41）A．DES B.RC-5 C.IDEA D.RSA

●(2009、2005年上)两个公司希望通过Internet传输大量敏感数据，从信息源到目的地之间的传输数据以密文形式出现，而且不希望由于在传输结点使用特殊的安全单元而增加开支，最合适的加密方式是 (46) ，使用会话密钥算法效率最高的 (47) 。

（46）A．链路加密 B.结点加密 C.端--端加密 D.混合加密

（47）A．RSA B.RC-5 C.MD5 D.ECC

●(2010年上)以下关于加密算法的叙述中，正确的是（43） 。

（43）A．DES算法采用128位的密钥进行加密 B．DES算法采用两个不同的密钥进行加密

C．三重DES算法采用3个不同的密钥进行加密 D．三重DES 算法采用2个不同的密钥进行加密

●(2011年下)公钥体系中，用户甲发送给用户乙的数据要用 （46） 进行加密。

（46）A. 甲的公钥 B. 甲的私钥 C. 乙的公钥 D. 乙方私钥

●(2012年下)3DES是一种 (44) 算法。

(44) A．共享密钥 B．公开密钥 C．报文摘要 D．访问控制

●(2013年上)利用三重DES进行加密，以下说法正确的是（41) 。

(41) A.三重DES的密钥长度是56位 B.三重DES使用三个不同的密钥进行三次加密

C.三重DES的安全性高于DES D.三重DES的加密速度比DES加密速度快

●(2013年下)下面算法中，不属于公开密钥加密算法的是（45） 。

（45）A.ECC B.DSA C.RSA D.DES

●(2014年上)高级加密标准AES支持的3种密钥长度中不包括 (41) 位。

（41）A.56 B.128 C.192 D.256

●(2015年上)以下关于三重DES加密的叙述中，正确的是 (45) 。

(45)A.三重DES加密使用一个密钥进行三次加密 B.三重DES加密使用两个密钥进行三次加密

C.三重DES加密使用三个密钥进行三次加密 D.三生EDS加密的密钥长度是DES密钥长度的3倍

●(2017年上)三重DES加密使用 (41) 个密钥对明文进行3次加密，其密钥长度为 (42) 位。

(41)A.1 B.2 C.3 D.4 (42)A.56 B.112 C.128 D.168

●(2017年上)以下加密算法中，适合对大量的原文消息进行加密传输的是 (43) 。

(43)A.RSA B.SHA-l C.MD5 D.RC5

●(2018年上)在安全通信中，A将所发送的信息使用（40）进行数字签名，B收到该消息后可利用（41）验证该消息的真实性。

（40）A.A的公钥 B.A的私钥 C.B的公钥 D.B的私钥

（41）A.A的公钥 B.A的私钥 C.B的公钥 D.B的私钥

●(2018年上)DES是一种（44）加密算法，其密钥长度为56位，3DES是基于DES的加密方式，对明文进行3次DES操作，以提高加密强度，其密钥长度是（45）位。

（44）A.共享密钥 B.公开密钥 C.报文摘要 D.访问控制

（45）A.56 B.112 C.128 D.168

●(2019年上)DES是 (7) 算法。

(7)A.公开密钥加密 B.共享密钥加密 C.数字签名 D.认证

# 实体认证

**认证分为实体认证和消息认证两种。实体认证是识别通信对方的身份（故又称为身份认证），防止假冒，可以使用数字签名的方法。消息认证是验证消息在传送或存储过程中有没有被篡改，通常使用报文摘要(消息摘要)的方法。本节主要分析实体认证。**

## 基于共享密钥的认证

**基于共享密钥的常见认证协议有：质询-回应协议、使用密钥分发中心的认证协议、Needham-Schroeder认证协议和Otway-Rees认证协议。**

### Needham-Schroeder认证协议

针对重放攻击，有以下几种解决方案：

#### **在每条消息中包含一个过期时间戳。**接收者检查消息中的时间戳，如果发现过期，则将消息丢弃。但是在网络上的时钟很难做到精确同步，所以时间戳的定义不好把握。定得太宽松，则容易遭受重放攻击；定得太紧凑，则消息容易过期。

#### **在每条消息之中放置临时值。**每一方必须要记住所有此前出现过的临时值，如果某条消息中再次包含了以前用过的临时值，则丢弃该消息。但是这样需要保存大量的临时值，而且机器有可能因某些原因丢失所有的临时值信息，从而遭受重发攻击。可以采用将时间戳和临时值结合起来的方式，以便减少需要记录的临时值，但协议实现稍微有些复杂。

#### 采用较为复杂的多路质询——回应认证协议，其中的典型是Needham-Schroeder认证协议。

该协议的实现过程如图 3.1所示。

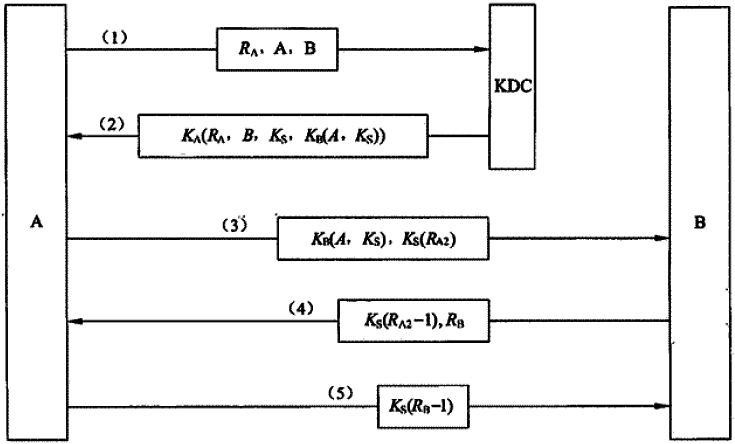


图 3.1 Needham-Schroeder认证协议

##### A想和B通信，首先产生一个大的随机数作为临时值，向KDC发送消息**M(RA，A，B)**。

##### KDC产生一个会话密钥KS，再用B的密钥KB加密(A,KS)，作为下轮A发给B的**票据KB（A，KS）**，然后再用A的密钥KA加密（RA，B，KS，KB(A，KS)）发送给A。

此步骤可理解为：KDC对A说：“A，KS是你要和B传递数据的会话密钥，以后你若能用KS解密一个加密包，则此加密包肯定是B发给你的。另外，请将信件KB(A，KS)交给B，B是我好朋友，见信如见人，B看到信后会关照你的！”。

##### A用自己的密钥KA解密密文，获取KS和KB(A，KS)，然后产生一个新的随机数RA2，用KDC发过来的KS加密RA2，将票据KB(A，KS)和KS(RA2)发给B；

##### B接收到消息用自己的密钥KB解密密文KB(A，KS)得到KS，再用KS解密密文KS(RA2)得到RA2；然后用KS加密（RA2-1）并产生随机数RB，再发回给A。

此步骤可理解为：KDC对B说：“B，KS是你要和A传递数据的会话密钥，以后你就用KS悄悄和A通信哈！”。

##### **A收到消息后确认了B的身份**，再向B发送KS（RB-1），**B收到消息后也可以确认A的身份**。

在该协议中，每一方都生成一个质询，并且回应一个质询，因此消除了任何一种重放攻击的可能性。

## 基于公钥的认证

基于公钥的认证采用公钥体制，通信的双方在发送通信消息时，都使用对方的公钥加密，并用各自的私钥对收到的消息解密，以判断通信用户的真实性。认证过程如图 3.2所示。

##### A首先生成质询信息RA，RA是一个随机数。接着A用B的公钥KB加密会话信息{A，RA}，然后发给B。

##### B用自己的私钥解出{A，RA}，再生成质询信息RB和会话密钥Ks，接着B用A的公钥KA加密会话信息{RA，RB，KS}，然后发给A。

##### A用自己的私钥解出{RA，RB，KS}，核对RA无误后（**此刻可断定和A通信的确实是B**），用KS加密RB，然后发给B。B收到后KS解出RB，B核实收到的RB和自己保留的RB，**如果无误，则能断定和B通信的确实是A，此时完成双向认证**。

**基于公钥的认证具有较高的安全性，由于通信前，通信双方都会产生一个随机数，排除了重放的可能性。**但是对于公钥的管理需要较高的代价，双方通信之前都须知道对方的公钥，通信方必须记录所有与之通信的其他通信方的公钥。

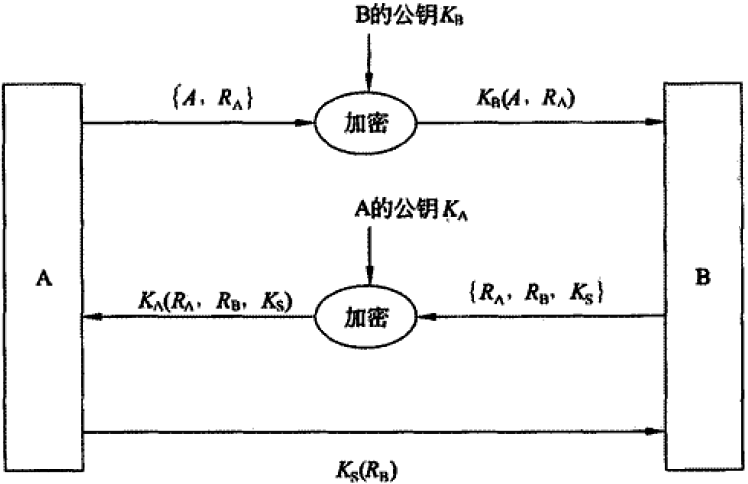


图 3.2基于公钥的认证

## 历年试题

●(2007年下)Needham-Schroeder协议是基于（41） 的认证协议。

（41）A.共享密钥 B.公钥 C.报文摘要 D.数字证书

# 数字签名

与人们手写签名的作用一样，数字签名系统向通信双方提供服务，使得A向B发送签名的消息P，以便达到：

B可以验证消息P确实来源于A(P使用A的私钥加密)；

A以后不能否认发送过P；

B不能编造或改变消息P。

数字签名的缺陷是不能确认接收方的身份，也不能保证接收方就一定能收到数据。目前应用广泛的数字签名算法主要有三种，即RSA签名、DSS签名和Hash签名。

## 基于共享密钥的数字签名

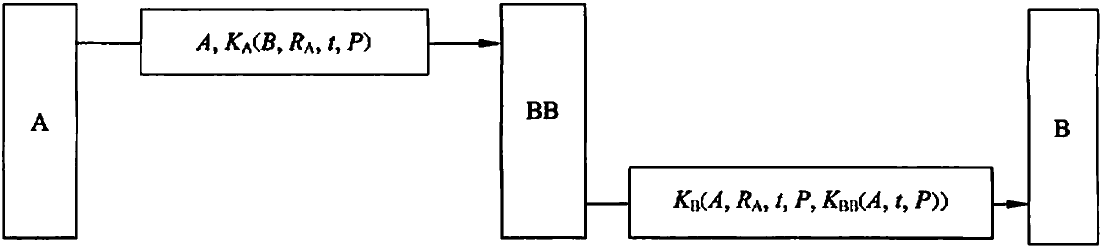


图 4.1基于共享密钥的签名

如图 4.1所示，设BB是A和B共同信赖的仲裁人。KA和KB分别是A和B与BB之间的共享密钥，而KBB是只有BB掌握的密钥，P是A发给B的消息，t是时间戳。BB解读了A的报文{A，KA（B，RA，t，P）}以后产生了一个签名的消息KBB（A，t，P），并装配成发给B的报文{KB（A，RA，t，P，KBB（A，t，P））}。B可以解密该报文，阅读消息P，并保留证据KBB（A，t，P）。由于A和B之间的通信是通过中间人BB的，所以不必怀疑对方的身份。又由于证据KBB（A，t，P）的存在，A不能否认发送过消息P，B也不能改变得到的消息P，因为BB仲裁人是可能会当场解密KBB（A，t，P），得到发送人、发送时间和原来的消息P。

## 基于公钥（非对称密钥）的数字签名

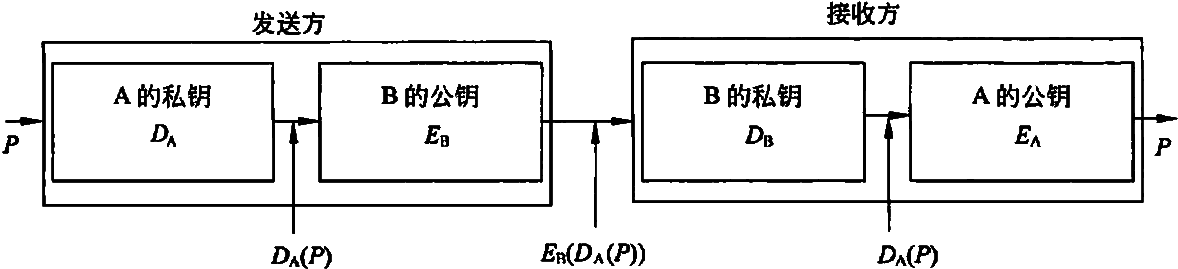


图 4.2基于公钥的数字签名

如图 4.2所示，A用自己的私钥DA加密消息P得DA(P)，再使用B的公钥EB加密DA(P)的EB(DA(P))并发送给B，B接收加密包以后使用自己的私钥DB解密EB(DA(P))得DA(P)，并将DA(P)作为证据保存，最后使用A的公钥EA解密DA(P)得明文P。

如果A否认了，B可以拿出证据DA（P），并用A的公钥EA解密得到P，从而证明P是A发送的。如果B把消息P篡改了，当A要求B拿出原来的DA（P），B拿不出来。

## 历年试题

●(2005年下)下面关于数字签名的说法错误的是(35)。

（35）A.能够保证信息传输过程中的保密性 B.能够对发送者的身份进行认证

C.如果接收者对报文进行了篡改，会被发现 D.网络中的某一用户不能冒充另一用户作为发送者或接收者。

●(2008年下)数字签名功能不包括 （42） 。

（42）A.防止发送方的抵赖行为 B.发送方身份确认 C.接收方身份确认 D.保证数据的完整性

●(2009年上)Alice向Bob发送数字签名的消息M，则不正确的说法是 (43) 。

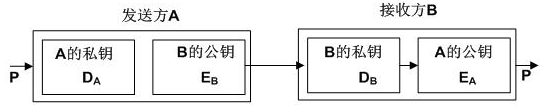
（43）A．Alice可以保证Bob收到消息M B．Alice不能否认发送过消息M

C．Bob不能缔造或改变消息M D．Bob可以验证消息M确实来源于Alice

●(2009年上)网络安全包含了网络信息的可用性、保密性和完整性和网络通信对象的真实性，其中数字签名是对（8）的保护。

（8）A.可用性 B.保密性 C.连通性 D.真实性

●(2011年上)下图所示为一种数字签名方案，网上传送的报文是 （43） ，防止A抵赖的证据是 （44） 。



（43）A. P B. DA(P) C. EB(DA(P)) D. DA

（44）A. P B. DA(P) C. EB(DA(P)) D. DA

●(2012年上)甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用（44）验证该消息的真实性。

(44)A．甲的公钥 B．甲的私钥 C．乙的公钥 D．乙的私钥

●(2016年下)下面不属于数字签名作用的是 (43) 。

(43)A.接收者可验证消息来源的真实性 B.发送者无法否认发送过该消息

C.接收者无法伪造或篡改消息  **D.可验证接受者的合法性**

# 数字证书

由于公开密钥体制的公钥是对所有人公开的，从而免去了密钥的传递，简化了密钥的管理，但是这个公开性在给人们带来便利的同时，也使攻击者冒充身份篡改公钥有了可乘之机。所以，**密钥也需要认证，在拿到某人的公钥时，需要先辨别一下它的真伪，这时就需要一个认证机构CA，将身份证书作为密钥管理的载体，并配套建立各种密钥管理设施。**

## 数字证书

**数字证书（Digital Certificate）又称为数字标识（Digital ID），提供一种在Internet上验证身份的方式，用来标识和证明网络通信双方身份的数字信息文件。**其**由第三方机构即CA中心签发**。

ITU的X.509数字证书包含如下的内容：

* 证书的版本号
* 证书的序列号
* 证书所使用的签名算法标识符
* 证书的发行机构名称
* 证书的有效期
* 证书所有人的名称
* 证书所有人的公开密钥及相关参数
* 证书发行机构ID
* 证书所有人ID
* 扩展域
* **证书发行机构对证书的签名**

在使用数字证书的过程中，通过运用对称和非对称密码体制等密码技术建立起一套严密的身份认证系统，能够保证以下要求：

信息除发送方和接收方外不被其他人窃取；

信息在传输过程中不被篡改；

发送方能够通过数字证书来确认接收方的身份；

发送方对于自己发送的信息不能抵赖。

## 认证中心CA

**CA(Certificate Authority，认证中心)作为权威的、可信赖的、公正的第三方机构，专门负责发放并管理所有参与网上交易的实体所需的数字证书。**其主要职责如下：

* 颁发证书；
* 管理证书；
* 用户管理；
* 吊销证书；
* 验证申请者信息；
* 保护证书服务器；
* 保护CA私钥和用户私钥；
* 审计和日志检查。

**死记住：**数字证书采用公钥体制进行加密和解密。每个用户有一个私钥，用它进行解密数据和数字签名；同时每个用户还有一个公钥，用于加密数据和验证信息的发送者身份。

## 历年试题

●(2004年上)RSA是一种基于(31)原理的公钥加密算法。网络上广泛使用的PGP协议采用RSA和IDEA两种加密算法组成链式加密体系，这种方案的优点是 (32) ，PGP还可以对电子邮件进行认证，认证机制是用MD5算法产生(33)位的报文摘要，发送方用自己的RSA私钥对 (34) 进行加密，附加在邮件中进行传送。如果发送方要向一个陌生人发送保密信息，又没有对方的公钥，那么他可以 (35) 。

(31)A．大素数分解　 B．椭圆曲线 C．背包问题　　 D．离散对数

(32)A．两种算法互相取长补短，从而提高了信息的保密性 B．可以组合成一种新的加密算法，从而避免专利技术的困扰

C．既有RSA体系的快捷性，又有IDEA算法的保密性 D．既有RSA体系的保密性，又有IDEA算法的快捷性

(33)A.256 B.60 C.128 D.96

(34)A．邮件明文　 B．IDEA密钥 C．邮件明文和报文摘要 D．报文摘要

(35)A．向对方打电话索取公钥　B．从权威认证机构获取对方的公钥C．制造一个公钥发给对方　D．向对方发一个明文索取公钥

●(2004年下)数字证书采用公钥体制进行加密和解密。每个用户有一个私钥，用它进行(46)；同时每个用户还有一个公钥，用于(47)。X.509标准规定，数字证书由(48) 发放，将其放入公共目录中，以供用户访问。

X.509数字证书中的签名字段是指(49)。如果用户UA从A地的发证机构取得了证书，用户UB从B地的发证机构取得了证书，那么(50)

（46）A.解密和验证　　　B.解密和签名　　　C.加密和签名　　 D.加密和验证

（47）A.解密和验证　　　B.解密和签名　　　C.加密和签名　　 D.加密和验证

（48）A.密钥分发中心　　B.证书授权中心　　C.国际电信联盟　 D.当地政府

（49）A.用户对自己证书的签名B.用户对发送报文的签名C.发证机构对用户证书的签名D.发证机构对发送报文的签名

（50）A.UA可使用自己的证书直接与UB进行安全通信 B.UA通过一个证书链可以与UB进行安全通信

C.UA和UB还须向对方的发证机构申请证书，才能进行安全通信

D.UA和UB都要向国家发证机构申请证书，才能进行安全通信

●(2009年上)在X.509标准中，不包含在数字证书中的数据域是(45)。

（45）A．序列号 B．签名算法 C．认证机构的签名 D．私钥

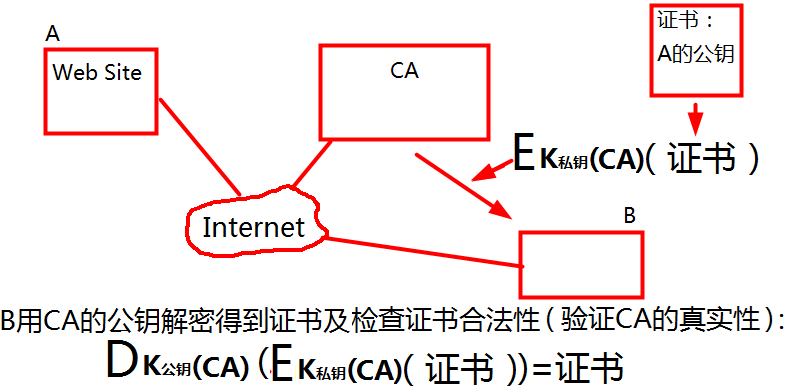
●(2009年下)某网站向CA申请了数字证书。用户通过（44）来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过（45）进行加密和验证，该网站通过（46）进行解密和签名。

（44）A．CA的签名 B．证书中的公钥 C．网站的私钥 D．用户的公钥

（45）A．CA的签名 B．证书中的公钥 C．网站的私钥 D．用户的公钥

（46）A．CA的签名 B．证书中的公钥 C．网站的私钥 D．用户的公钥

解析：



在以上图解中，如果B使用证书上的公钥去解密来自于A的加密包，能成功解密即能确认对方身份就是A。

●(2010年下)公钥体系中，私钥用于（49） ，公钥用于（50） 。

（49）A.解密和签名 B.加密和签名 C.解密和认证 D.加密和认证

（50）A.解密和签名 B.加密和签名 C.解密和认证 D.加密和认证

●【2011年上】用户A从CA获得用户B的数字证书，并利用 （7） 验证数字证书的真实性。

（7）A.B的公钥 B.B的私钥 C.CA的公钥 D.CA的私钥

●(20011年下)从认证中心CA获取用户B的数字证书，该证书用（9） 作数字签名；从用户B的数字证书中可以获得B的公钥。

（9）A.CA的公钥 B.CA的私钥 C.B的公钥 D.B的私钥

●(2012年下)用户B收到用户A带数字签名的消息M，为了验证M的真实性，首先需要从CA获取用户A的数字证书，并利用(42)验证该证书的真伪，然后利用(43)验证M的真实性。

(42) A. CA的公钥 B.B的私钥 C.A的公钥 D.B的公钥

(43) A. CA的公钥 B.B的私钥 C. A的公钥 D.B的公钥

●(2014年下)假设有证书发放机构I1、I2，用户A在I1获取证书，用户B在I2获取证书，I1和I2己安全交换了各自的公钥，如果用I1《A》表示由I1颁发给A的证书，A可通过 (41) 证书链获取B的公开密钥。

(41)A.I1《I2》I2《B》 B.I2《B》Il《I2》 C.I1《B》I2《I2》 D.I2《I1》I2《B》

●(2017年上)假定用户A、B分别在和两个CA处取得了各自的证书，下面 (44) 是 A、B 互信的必要条件。

(44)A.A、B互换私钥 B.A、B互换公钥 C.、互换私钥 D.、互换公钥

●(2019年上)用户 A 和 B 要进行安全通信，通信过程需确认双方身份和消息不可否认，A、B 通信时可使用 （43） 来对用户的身份进行认证，使用 （44） 确保消息不可否认。

（43）A、数字证书 B、消息加密 C、用户私钥 D、数字签名

（44）A、数字证书 B、消息加密 C、用户私钥 D、数字签名

●(2019年上)非对称加密算法中，加密和解密使用不同的密钥，下面的加密算法中 （41） 属于非对称加密算法。若甲、乙采用非对称密钥体系进行保密通信，甲用乙的公钥加密数据文件，乙使用 （42） 来对数据文件进行解密。

（41）A、AES B、RAS C、IDEA D、DES

（42）A、甲的公钥 B、甲的私钥 C、乙的公钥 D、乙的私钥

# 密钥管理

密钥管理是指**处理密钥自产生到最终销毁的整个过程中的有关问题，包括系统的初始化，密钥由产生、存储、备份，恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁。**

密钥管理是信息安全的核心技术之一，主要有三种：

#### 适用于封闭网的技术，以传统的密钥分发中心为代表的KMI机制；

#### 适用于开放网的PKI机制；

#### 适用于规模化专用网的SPK技术。

## KMI技术

**密钥管理基础结构（Key Management Infrastructure，KMI）假定有一个密钥分发中心(KDC)来负责发放密钥。**这种结构经历了从静态分发到动态分发的发展历程，**目前仍然是密钥管理的主要手段**。无论是静态分发还是动态分发，都是基于秘密的物理通道进行的。

## PKI技术

公钥基础结构（Public Key Infrastructure，PKI）是**运用公钥的概念和技术**来提供安全服务的、普遍适用的网络安全基础设施，包括由PKI策略、软硬件系统、认证中心、注册机构（Registration Authority，RA)、证书签发系统和PKI应用等构成的安全体系。

## 历年试题

●(2006年上) (38)不属于PKI CA(认证中心)的功能。

(38)A. 接收并验证最终用户数字证书的申请 B. 向申请者颁发或拒绝颁发数字证书

C. 产生和发布证书废止列表(CRL)，验证证书状态 D. 业务受理点LRA 的全面管理

解析：LRA(Local Registration Authority):分支机构的证书申请受理点。

●(2013年下)PKI体制中，保证数字证书不被篡改的方法是（43） 。

（43）A.用CA的私钥对数字证书签名 B.用CA的公钥对数字证书签名

C.用证书主人的私钥对数字证书签名 D.用证书主人的公钥对数字证书签名

# 消息摘要

消息摘要的产生源于**保证数据完整性的安全需求**。消息摘要算法的主体就是设计单向的Hash函数。单向散列函数H(M)作用于一个任意长度的数据M，它返回一个固定长度(m)的散列h,h称为数据M的摘要。**单向散列函数**的特点有：

* 可用于任意大小的数据块；
* 能产生固定大小的输出；
* 软/硬件容易实现；
* **给定M，很容易计算h(h=H(M))；**
* **给定h，无法推算出M**
* **给定M，找不到另一个数据N，使得H(M)=H(N)**

## 常用的消息摘要算法

MD5算法

MD5是RSA数据安全公司开发的一种**单向散列算法**。已经被广泛使用，可以把不同长度的数据块进行编码（以512位的分组进行处理）成一个**128位的散列值**。

安全散列算法（SHA）

SHA（The Secure Hash Algorithm）可以对任意长度的数据运算成一个**160位的散列值**。此算法缺点是比MD5慢，但是报文摘要更长，更有利于抵抗野蛮攻击。

散列式报文认证码

散列式报文认证码(Hashed Message Authentication Code，HMAC)是利用对称密钥生成报文认证码的散列算法，可以提供数据完整性数据源身份认证。

## 历年试题

●(2009年上)安全散列算法SHA-1产生在摘要的位数是 (44) 。

（44）A．64 B．128 C．160 D．256

●(2010年下)报文摘要算法MD5的输出是（45）位，SHA-1的输出是（46）位。

（45）A.56 B.128 C.160 D.168

（46）A.56 B.128 C.160 D.168

●(2011年上)下列选项中，同属于报文摘要算法的是 42）。

（42）A. DES和MD5 B. MD5和SHA-1 C. RSA和SHA-1 D. DES和RSA

●(2011年下，2017年上)某报文的长度是1000字节，利用MD5计算出来的报文摘要长度是（41）位，利用SHA计算出来的报文摘要长度是（42）位。

（41）A.64 B.128 C.256 D.160

（42）A.64 B.128 C.256 D.160

●(2012年上)下列算法中，（45）属于摘要算法。

(45)A．DES B．MD5 C．Diffie-Hellman D．AES

●（2013年上）利用报文摘要算法生成报文摘要的目的是（42) 。

(42) A.验证通信对方的身份，防止假冒 B.对传输数据进行加密，防止数据被窃听

C.防止发送方否认发送过的数据 D.防止发送的报文被篡改

●（2013年下）报文摘要算法SHA-1输出的位数是（44）。

（44）A.100位 B.128位 C.160位 D.180位

●(2014年上)在报文摘要算法MD5中，首先要进行明文的分组与填充，其中分组时明文报文要按照 (42)位分组。

（42）A.128 B.256 C.512 D.1024

●(2015年下)下列算法中，可用于报文认证的是（42），可以提供数字签名的是（43）。

（42）A.RSA B.IDEA C.RC4 D.MD5

（43）A.RSA B.IDEA C.RC4 D.MD5

# 无线局域网安全协议

## WLAN安全协议

IEEE正致力于解决WLAN的安全问题，最初使用**WEP协议**，但WEP并不能使那些重要信息免遭恶意攻击，之后出现了**WPA协议**，它弥补了WEP中的大多数缺陷，但也并非完美，目前**WPA2(WPA，第二版本)**在广泛使用，它是Wi-Fi联盟对采用IEEE 802.11i安全增强功能产品的认证计划，也可以看成WEP的升级版。

WEP

WEP（Wired Equivalent Privacy，有线等效保密）协议采用**对称密钥方式来处理数据报的加密和解密**，其**核心RC4算法是一种流式加密算法**，它将短的密钥值展开成为无限长的伪随机比特流，发送者使用这个伪随机比特流与明文数据做异或操作来产生密文。**WEP加密密钥为40位。**

WPA

WPA（Wi-Fi Protected Access，Wi-Fi网络保护访问）是Wi-Fi联盟为了弥补WEP缺陷采用的最新安全标准。

WPA采用TKIP（Temporal Key Integrity Protocol，暂时密钥完整协议）和IEEE 802.1x来实现WLAN的访问控制、密钥管理和数据加密。

TKIP仍然基于RC4加密，每个用户每次通信只用一次WEP密钥，加密密钥的长度为104位。

802.11i

802.11i是IEEE802.i协议标准的扩展，取代传统的WEP加密技术，其采取的加密算法是**AES**。

## 历年试题

●(2008年上)设置计算机的无线网卡，使该计算机与实验室的无线访问点LabAP之间的通信能够受密码保护，指定密钥为2350AD9FE0，则下图中应设置（43）

（43）A.SSID为LabAP，网络验证为开放式，数据加密为WEP

B.SSID为2350AD9FE0，网络验证为开放式，数据加密为WEP

C.SSID为LabAP，网络验证为WEP，数据加密为开放式

D.SSID为2350AD9FE0，网络验证为WEP，数据加密为开放式



●(2010年下)IEEE 802.11i所采用加密算法是为（48） 。

（48）A.DES B.3DES Ｃ.IDEA D.AES

●(2013年下)在Wi-Fi安全协议中，WPA与WEP相比，采用了一些（60) 。

(60)A.较短的初始化向量 B.更强的加密算法 C.共享密钥认证方案 D.临时密钥以减少安全风险

●(2015年上)为了弥补WEP协议的安全缺陷，WPA安全认证方案增加的机制是 (52) 。

(52)A.共享密钥认证 B.临时密钥完整性协议 C.较短的初始化向量 D.采用更强的加密算法

●(2017年下)无线局域网通常采用的加密方式是WPA2，其安全加密算法是 (44) 。

(44)A.AES和TKIP B.DES和TKIP C.AES和RSA D.DES和RSA

# 虚拟专用网VPN

**VPN（Virtual Private Network）,建立在公用网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对VPN用户之间没有专用的物理连接，而是通过ISP提供的公用网络来实现通信的，其专用性表现在VPN之外的用户无法访问VPN内部的网络资源，VPN内部用户之间可以实现安全通信。**这里讲的VPN是指在Internet上建立的、由用户(组织或个人)自行管理的VPN，而不涉及一般电信网中的VPN。后者一般是指X.25、帧中继或ATM虚拟专用线路。

目前VPN主要采用四项技术来保证安全，分别:**隧道技术(Tunneling)、加解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)。**

**VPN使用的隧道协议主要有第二层隧道协议、第三层隧道协议和高层隧道协议。**

## 第二层隧道协议

第二层隧道协议有**PPTP、L2F，L2TP和MPLS（Multi-Protocol Label Switching, 多协议标记交换）**。L2TP协议是目前IETF的标准，由IETP在PPTP和L2F的基础上发展而成。**第二层隧道协议是先把各种网络协议封装到PPP中**，再把整个数据包封装到隧道协议中，形成的数据包依靠第二层协议进行传输。

PPP协议

PPP协议建立起物理层连接之后，将在数据链路层连接阶段进行用户验证，目前较常用的口令是口令验证协议（PAP）和挑战握手验证协议（CHAP）.

##### PAP身份认证

PAP（Password Authentication Protocol，密码认证协议）的身份认证是两次握手验证过程，口令以明文形式传输。过程如图 9.1所示：

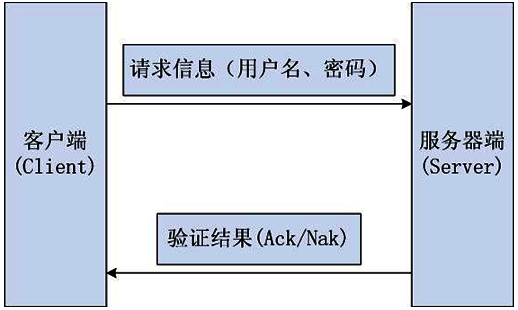


图 9.1 PAP认证过程

##### CHAP身份认证

CHAP（Challenge Handshake Authentication Protocol，挑战握手认证协议）是一种加密的验证方式，**采用三次握手验证**，服务器端存有客户的明文口令。过程如图 9.2所示：



图 9.2 CHAP认证过程

##### PAP认证和CHAP认证的区别

PAP采用二次握手机制实现，身份验证时密码以明文传输，不能防止重放攻击，因此安全性不高。

CHAP采用三次握手机制，可实现双向验证。密码不直接在网络上传输，通过使用唯一的、不可预知的、可变的挑战消息来防止回放攻击。CHAP不但在建立链路之时可进行验证，而且在链路建立后的任何时候都可以进行重复验证。

PPTP隧道协议

PPTP（Point to Point Tunneling Protocol），即点对点隧道协议。该协议是在PPP协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网（VPN），可以通过密码验证协议（PAP）、可扩展认证协议（EAP）等方法增强安全性。其封装如图 9.3所示。



图 9.3 PPTP封装图

L2TP隧道协议

L2TP是一种工业标准的Internet隧道协议，功能大致和PPTP协议类似，比如同样可以对网络数据流进行加密。但PPTP要求网络为IP网络，L2TP要求面向数据包的点对点连接；PPTP使用单一隧道，L2TP使用多隧道；L2TP提供包头压缩、隧道验证，而PPTP不支持。其对应的封装图如图 9.4所示。

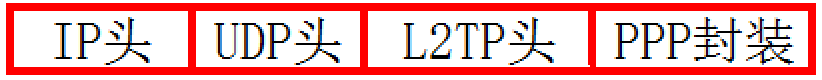


图 9.4 L2TP封装图

## 第三层IPSec隧道协议

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。**第三层隧道协议有VTP、IPSec、GRE等，其中IPSec**定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。

### IPSec作用

IPSec（IP Security）用于增强IP网络的安全性，适用于网络层。IPSec协议集提供了下面的安全服务：

数据完整性（Data Integrity）

保持数据的一致性，防止未授权地生成、修改或删除数据。

认证（Authentication）

保证接收的数据与发送的相同，保证实际发送者就是声称的发送者。

保密性（Confidentiality）

传输的数据是经过加密的，只有预定的接收者知道发送的内容；

应用透明的安全性（Application-transparent Security）

IPSec的安全头插入在标准的IP头和上层协议（例如TCP）之间，任何网络服务和网络应用可以不经修改地从标准IP转向IPSec，同时IPSec通信也可以透明地通过现有的IP路由器。

IPSec的功能可划分为如下的三类：

* 认证头（Authentication Head，AH）：用户数据完整性认证和数据源认证,不能加密数据；
* 封装安全负荷（Encapsulation Security Payload，ESP）：提供数据保密性和身份认证(数据源认证)，ESP也包括了防止重放攻击的顺序号。
* Internet密钥交换协议（Internet Key Exchange，IKE）：用于生成和分发在ESP和AH中使用的密钥，IKE也对远程系统进行初始认证。

### 安全关联SA

**SA（Security Association，安全关联）是IPSec的基础，它为两个使用IPSec的实体（主机或路由器）建立单向的逻辑连接**，定义了实体间安全服务的具体细节（如采用的IPSec安全协议、散列方式、加密算法和密钥等安全参数）。

**SA是单向的，所以两个实体之间的双向通信至少需要建立两个SA，一个为数据流出SA，一个为数据流入SA**。

SA由一个三元组唯一地确定，它们是：<安全参数索引SPI，目标IP地址，安全协议>。描述如下：

* SPI: 一个 32 位的连接标识符，称为安全参数索引 SPI (Security Parameter Index)；
* 目标IP地址: 此单向连接的目的 IP 地址（SA的目的地址）；
* 安全协议的标识符（说明使用的是AH或ESP）。

### 认证头AH

**IPSec认证头提供了数据完整性和数据源认证，但是不提供保密服务。**AH包含了对称密钥的散列函数。使得第三方无法修改传输中的数据。IPSec支持下面的认证算法：

* HMAC-SHAI（Hashed Message Authentication Code-Secure Hash Algorithm 1)，160位密钥。
* HMAC-MD5（HMAC-Message Digest 5)，128位密钥。

IPSec有两种模式：**传输模式(端点到端点之间IPSec VPN,不需要新的IP头)和隧道模式（需要新的IP头，网络到网络之间的VPN）**。

在传输模式中，IPSec认证头插入原来的lP头之后（如图 9.5所示），IP数据和IP头用来计算AH认证值。

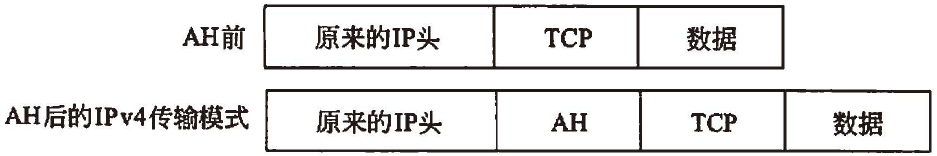


图 9.5传输模式的认证头

在隧道模式中，IPSec用新的IP头封装原来的IP数据报（包括原来的IP头），原来的IP数据报的所有字段都经过了认证，如图 9.6所示。



图 9.6隧道模式的认证头

### 封装安全负载ESP

**IPSec封装安全负荷提供了数据加密功能。**ESP利用对称密钥对IP数据（例如TCP包）进行加密，支持的加密算法如下：

* DES-CBC（Data Encryption Standard Cipher Block Chaining Mode），56位密钥。
* 3DES-CBC（三重DES-CBC），2个56位密钥。
* AES128-CBC（Advanced Encryption Standard CBC），128位密钥。

在传输模式下，IP头没有加密，只对IP数据进行加密，如图 9.7所示：

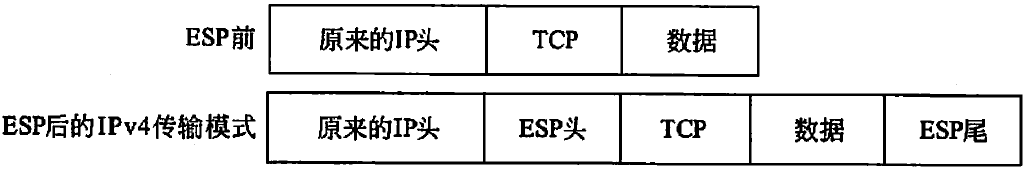


图 9.7传输模式中的ESP

在隧道模式，IPSec对原来的IP数据报进行了封装和加密，加上了新的IP头，如图 9.8所示。

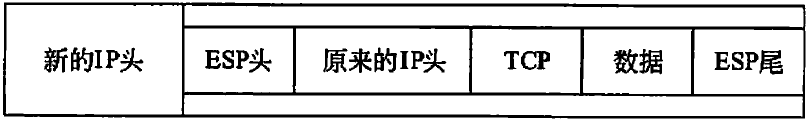


图 9.8隧道模式的ESP

### 带认证的封装安全负载(ESP)

ESP加密算法本身没有提供认证功能，不能保证数据的完整性。但是带认证的ESP可以提供数据完整性服务。有如下两种方法可提供认证功能。

#### **带认证的ESP。**IPSec使用第一个对称密钥对负荷进行加密，然后使用第二个对称密钥对经过加密的数据计算认证值，并将其附加在分组之后，如图 9.9所示。

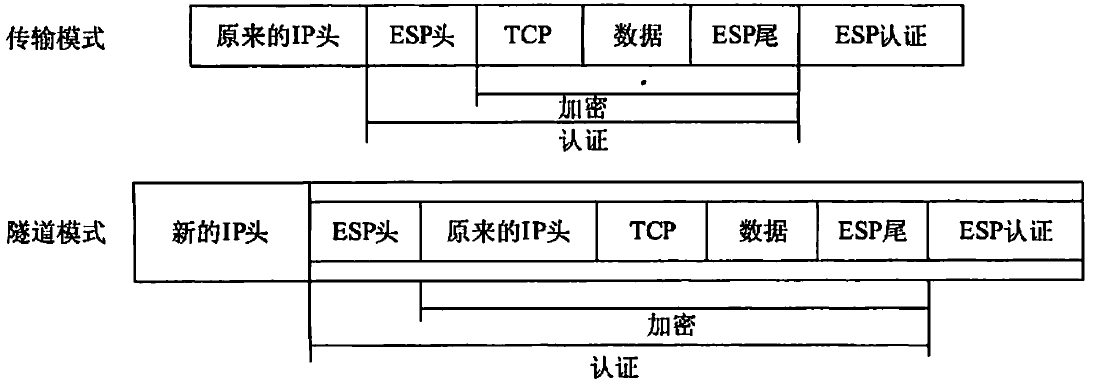


图 9.9带认证的ESP

#### **在AH中嵌套ESP。**ESP分组可以嵌套在AH分组中，如图 9.10所示。

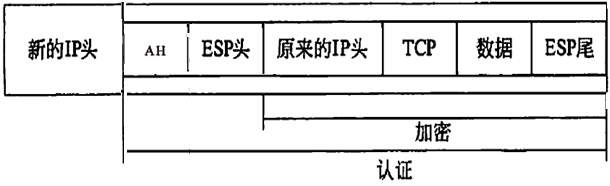


图 9.10在AH中嵌套ESP

### Internet密钥交换协议IKE

IPSec传送认证或加密的数据之前，必须就协议、加密算法和使用的密钥进行协商。密钥变换协议提供这个功能，并且在密钥交换之前还要对远程系统进行初始的认证。

IKE实际上是**ISAKMP**(Internet Security Association and Key Management Protocol)、Oakley和SKEME（Versatile Secure Key Exchange Mechanism for Internet protocol）这三个协议的混合体。ISAKMP提供认证和密钥交换的框架，但不给出具体的定义，Oakley描述密钥交换的模式，SKEME定义了密钥交换技术。在使用IKE协议时，需要定义IKE协商策略，该策略由ISAKMP/Oakley进行定义。

## 高层隧道协议

目前主要的高层隧道协议主要有**SSL/TLS、SOCKS**等。

### SSL/TLS协议

SSL（Secure Socket Layer，安全套接字层）协议是使用公钥和对称密钥技术，在浏览器和Web服务器之间构造安全通道来进行数据传输。SSL运行在TCP/IP层之上、应用层之下，即用于在传输层和应用层之间提供加密方案，为应用程序提供加密数据通道。

SSL协议的优势在于它是与应用层协议独立无关的。高层的应用层协议（例如：HTTP、FTP、Telnet等等）能透明的建立于SSL协议之上。

SSL首先在传输层中对网络通信数据进行加密，然后与应用层的协议相结合，在此之后应用层协议所传送的数据都会被加密，从而保证通信的私密性。

对SSL3.0协议进行进一步的扩展提出了TLS（Transport Layer Security，传输层安全协议），其主要的目标是在两个通信进程之间提供数据加密和数据完整性验证服务。

由于SSL和TLS3.0只有细微的差别，在不涉及差别的情况下，可以将SSL与TLS等价，合称为SSL/TLS。

SSL/TLS结合使用了对称密码技术和公开密码技术，可以实现如下三个通信目标：**数据加密、完整性验证、身份认证。**

**大多数Web交易均采用传统的HTTP协议，并使用经过SSL加密的HTTP报文来传输敏感的交易信息，此时访问Web应用需要使用“https://”（在传统“http://”基础上加一个“s”），默认的SSL端口号为443。**

**SSL不对应用层的数据进行数字签名，因此它不能保证信息的不可抵赖性。**

### SOCKS协议

**SOCKS是一种基于会话层的网络代理协议。SOCKS。它拥有在TCP和UDP领域为客户端/服务器应用程序提供一个框架，以方便安全地使用网络防火墙的服务。**

SOCKS协议提供一个框架。利用网络防火墙将组织内部的网络结构与外部网络（如Internet）有效地隔离开来。这些防火墙系统通常以应用层网关的形式工作在网络之间，提供受控TELNET、FTP和SMTP等接入服务。SOCKS提供通用框架使这些协议安全透明地穿过防火墙。

**SOCKS代理比其他应用层代码要快得多，通常绑定在代码服务器上的1080端口上。**

## 历年试题

●(2006年上)关于虚拟专用网，下面正确的语句是(25)。

(25)A.安全套接层协议(SSL)是在应用层和传输层之间增加的安全机制，可以用SSL在任何网络上建立虚拟专用网

B.安全套接层协议(SSL)的缺点是只进行服务器端对客户端的单向身份认证

C.安全IP协议(IPSec)通过认证头(AH)提供无连接的数据完整性和数据源认证、数据机密性保护和抗重发攻击服务

D.当IPSec 处于传输模式时，报文不仅在主机到网关之间的通路上进行加密，而且在发送方和接收方之间的所有通路上都要加密

●(2006年上)建立PPP 连接以后，发送方就发出一个提问消息(Challenge Message)，接收方根据提问消息计算一个散列值。(26)协议采用这种方式进行用户认证。

(26)A. ARP B. CHAP C. PAP D. PPTP

●(2006年上)以下用于在应用层和传输层之间提供加密方案的协议是 (36) 。

(36)A. PGP　B. SSL　C. IPSec 　D. DES

●(2006年下)IPSec VPN安全技术没有用到（35）。

（35）A. 隧道技术　　 B. 加密技术　　C. 入侵检测技术　　D. 身份认证技术

●(2007年下)实现VPN的关键技术主要有隧道技术、加解密技术、 （44） 和身份认证技术。如果需要在传输层实现VPN，可选的协议是 （45） 。

（44）A. 入侵检测技术 B. 病毒防治技术 C. 安全审计技术 D. 密钥管理技术

（45）A. L2TP B. PPTP C. TLS D. Ipsec

●(2008年上)下面的选项中，属于传输层安全协议的是（44）

（44） A.IPsec B.L2TP C.TLS D.PPTP

●(2008年上)（46）不属于电子邮件协议

（46）A.POP3 B.SMTP C.IMAP D.MPLS

●(2008年下)TCP/IP在多个层引入了安全机制，其中TLS协议位于 （9） 。

（9）A.数据链路层 B.网络层 C.传输层 D.应用层

●(2009年下)IPSec的加密和认证过程中所使用的密钥由 （47）机制来生成和分发。

（47）A．ESP B．IKE C．TGS D．AH

●(2010年下)下列隧道协议中工作在网络层的是（47） 。

（47）A.SSL B.L2TP C.IPSec D.PPTP

●(2012年下)下列安全协议中，与TLS功能相似的协议是(41)。

(41) A．PGP B．SSL C．HTTPS D．IPSec

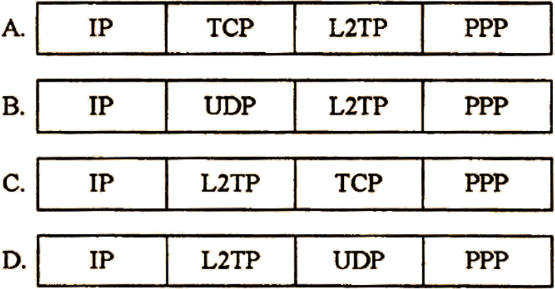
●(2012年下)IPSec中安全关联(Security Associations)三元组是 (45) 。

(45) A．<安全参数索引SPI，目标IP地址，安全协议> B．<安全参数索引SPI，源IP地址，数字证书>

C．<安全参数索引SPI，目标IP地址，数字证书> D．<安全参数索引SPI，源IP地址，安全协议>

●(2013年上)下面能正确表示L2TP数据包的封装格式的是（44) 。

(44)



●(2014年上)以下关于IPsec协议的描述中，正确的是 (43) 。

(43)A．IPsec认证头(AH)不提供数据加密服务 B．IPsec封装安全负荷(ESP)用于数据完整性认证和数据源认证

C．IPsec的传输模式对原来的IP数据报进行了封装和加密，再加上了新的IP头

D．IPsec通过应用层的Web服务建立安全连接

●(2017年上)IPSec用于增强IP网络的安全性，下面的说法中不正确的是 (39) 。

(39)A.IPSec可对数据进行完整性保护 B.IPSec提供用户身份认证服务

C.IPSec的认证头添加在TCP封装内部 D.IPSec对数据加密传输

# 应用层安全协议

## SSH（Secure Shell）协议

常用的应用层网络通信协议（如FTP、POP3和Telnet）大多数是不安全的，因为它们在网络上用明文传送用户名、口令和数据，很容易被窃听、假冒、篡改和欺骗。

**SSH是一种在不安全网络中用于安全远程登录和其他安全网络服务的协议。它提供了对安全远程登录、安全文件传输和安全TCP/IP及X-Windows系统通信量进行转发的支持。它可以加密、认证并压缩传输的数据。**

## S-HTTP

**安全的超文本传输协议（Secure HTTP，S-HTTP）**是一个面向报文的安全通信协议，是HTTP协议的扩展，其设计目的是保证商业贸易信息的传输安全，促进电子商务的发展。

S-HTTP与HTTP使用的语法相同，但报文格式不同，为了与HTTP报文区分，S-HTTP报文使用了协议指示器Secure-HTTP/1.4，这样S-HTTP报文可以与HTTP报文混合在同一个TCP端口（80）进行传输。

**由于SSL的迅速出现，S-HTTP未能得到广泛使用。目前SSL基本取代了S-HTTP。大多数Web交易均采用传统的HTTP协议，并使用经过SSL加密的HTTP报文来传输敏感的交易信息，此时访问Web应用需要使用“**错误!超链接引用无效。**s”（在传统“http://”基础上加一个“s”），默认的SSL端口号为443。**

## PGP（Pretty Good Privacy）协议

**PGP是1991开发的电子邮件加密软件包。**其特点如下：

* 能够在各种平台上（如DOS、Windows、UNIX等）免费使用，并得到许都制造商的支持；
* 基于比较安全的加密算法和散列算法（RSA、IDEA、MD5）；
* 具有广泛的应用领域，即可用于加密文件，也可用于个人安全通信；

PGP提供两种服务：**数据加密和数字签字。**

**数据加密机制可以应用于本地存储的文件，也可以应用于网络上传输的电子邮件。**

**数字签名机制用于**数据源身份认证和报文完整性验证。

PGP使用RSA公钥证书进行身份认证，使用IDEA(128位密钥)进行数据加密，使用MD5进行数据完整性验证。

**PGP进行身份认证的过程叫做公钥指纹（public-key fingerprint）。**所谓指纹，就是对密钥进行MD5变换后所得到的字符串。假如MD5能够识别Bob的声音，则Alice可设法得到Bob的公钥，并生成公钥指纹，通过电话验证他得到的公钥指纹是否与Bob的公钥指纹一致，以证明Bob公钥的真实性。

## S/MIME

**S/MIME（Secure/Multipurpose Internet Mail Extensions）是RSA数据安全公司开发的软件。**S/MIME提供的安全服务有报文完整性验证、数字签名和数据加密，其可以添加在邮件系统的用户代理中，用于**提供安全的电子邮件传输服务**，也可以加入其他的**传输机制（例如HTTP）中**，安全地传输任何MIME报文，甚至可以添加在自动报文传输代理中，在Internet中安全地传送由软件生成的FAX报文。

## 安全的电子交易

**安全的电子交易（Secure Electronic Transaction，SET）是一个安全协议和报文格式的集合**，融合了SSL、STT（Secure Transaction Technology）、S-HTTP以及PKI技术，通过数字证书和数字签名机制，使得客户可以与供应商进行安全的电子交易，是现代电子交易中的安全基础设施。

**SET提供了以下三种服务：**

* 在交易涉及的各方之间提供安全信道；
* 使用X.509数字证书实现安全的电子交易；
* 保证信息的机密性。

## Kerberos服务

**Kerberos不是建立一个精密的认证协议，而是提供一个集中的认证服务器，其功能是实现应用服务器与用户间的相互认证。**

**Kerberos协议的安全性不依赖于用户登录的主机或者应用服务器，而是依赖于Kerberos的认证服务器。**Kerberos可以防止**偷听和重放攻击，保护数据的完整性**。

Kerberos的安全机制如下：

* **AS(Authentication Server)：**认证服务器，其为用户发放TGT以便用户和TGS服务器进行交互；
* **TGS(Ticket Granting Server)：**票据授予服务器，负责发放用户访问应用服务器时需要的票据。**认证服务器和票据授予服务器组成密钥分发中心KDC（Key Distribution Center）；**
* V：用户请求访问的应用服务器；
* TGT（Ticket Granting Ticket）：用户向TGS证明自己身份的初始票据，**即KTGS（A，KS）**。

Kerberos的认证过程如图 10.1所示。

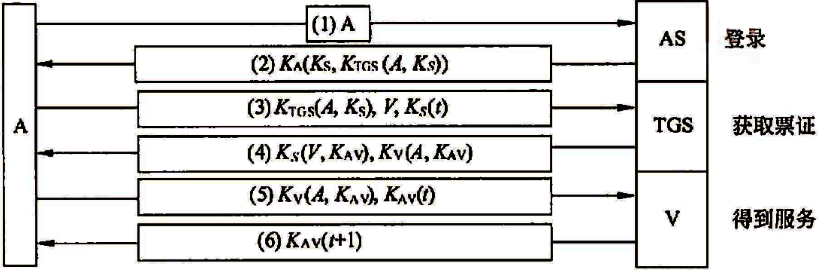


图 10.1 Kerberos服务

#### 用户A向KDC中的AS申请和TGS通信需要的初始票据**TGT=KTGS(A,KS)；**

#### AS验证用户A的真实性和访问权限后，向用户A发放TGT会话票据；

#### 用户向TGS请求和服务器V通信的会话票据；

#### TGS验证用户身份后发放给用户A会话票据KAV；

#### 用户A向应用服务器V请求登录；

#### 用于服务器向用户验证时间戳。

## RADIUS协议

**RADIUS（Remote Access Dail-In User Service）是对远程用户进行认证和记帐的一种协议。**是基于客户端/服务器端模式的安全协议，是目前实现AAA访问控制管理框架的最常用协议之一，其对用户进行认证、授权和计费功能，**默认认证使用端口UDP 1812，默认计费端口为UDP 1813。**

### RADIUS的基本描述

如图 10.2所示，RADIUS采用质询/响应(Challenge/Response)方式进行交互。在实体结构图中。RADIUS服务的客户端为NAS，服务端为RADIUS服务器。被配置为客户端的NAS一方面接收用户的信息，并要求终端用户响应其质询；另一方面响应RADIUS服务器的质询。

**RADIUS提供代理和漫游功能。**一台RADIUS服务器可以作为其他RADIUS服务器的代理设备转发RADIUS认证和计费数据报。使用代理功能，让用户在异地也可以通过其他的RADIUS服务器进行认证，从而实现**“漫游”**。

**RADIUS协议还制定了重传机制。**如果NAS向某个RADIUS服务器提交请求但没有收到回应，就可以向备份RADIUS服务器重传请求。由于允许多个备份RADIUS服务器存在，因此NAS进行重传时，可以采用轮询的方式。如果备份RADIUS服务器的密钥和主RADIUS服务器的密钥不同，就需要进行重新认证。



图 10.2 RADIUS实体结构图

### RADIUS的工作原理

RADIUS的基本工作流程如下。

#### 用户拨入NAS，向NAS发送用户名和口令。

#### NAS在收到用户的请求后，生成一个接入申请(Access Request)消息并发送给RADIUS服务器。该消息中包含有**用户名称、用户密码摘要、客户端ID和申请接入端口等字段**。**为了保证安全，用户密码不会直接在网络上传送，实际传送的只是使用MD5摘要算法计算出来的用户密码的消息摘要。**

#### 当RADIUS服务器收到接入申请消息后，提取出RADIUS服务器与NAS的共享密钥，检查NAS的合法性。如果NAS不合法，RADIUS服务器将丢弃该接入申请，如果NAS合法，RADIUS服务器将查找用户的数据库，根据接入申请消息中用户提供的认证信息与数据库中该用户的资料进行认证。

#### 如果接入申请消息中包含有属性为“代理”的内容，则RADIUS服务器将该消息转发给远程RADIUS服务器。当RADIUS服务器接收到远程RADIUS服务器的回应后，再将回应发送回NAS。

#### 当用户信息通过RADIUS服务器认证之后，若RADIUS服务器需要对用户进行进一步的验证，可发送一个接入**挑战报文(Access Challenge)消息给NAS**。NAS在收到接入挑战报文后，将提示用户进行回应。用户回应后，NAS再将新的接入申请消息发送给RADIUS服务器，新的接入申请消息中包含了用户对接入挑战报文的回应记录。**RADIUS服务器对接入申请消息进行检验，如果检验成功，则以接入许可(Access Accept)消息的形式将用户的权限信息发送给NAS)，如果检验失败，则将接入拒绝(Access-Reject)消息发送给NAS。**

#### 如果RADIUS服务器并不要求进一步的验证，可在第一次接入申请中，根据用户信息与数据库资料的认证结果，直接发送接入许可/拒绝消息给NAS。

#### NAS根据接收到的认证结果允许或拒绝用户接入。如果允许用户接入，则NAS向RADIUS服务器发送计费请求(Accounting-Request)消息，消息中status-type字段取值为start，表示要求RADIUS服务器开始计费。

#### RADIUS服务器返回计费开始响应(Accounting-Response)消息。

#### 用户开始访问资源。

#### 当用户即将结束访问，NAS向RADIUS服务器发送计费请求消息，消息中status-type字段取值为stop，表示要求RADIUS服务器停止计费。

#### RADIUS服务器返回计费结束响应消息。

#### 用户访问资源结束。

## IEEE802.1x协议

IEEE802.1x协议的全称是基于端口的访问控制协议（Port-based Network Access Control Protocol)。IEEE 802.1x协议起源于IEEE 802.11协议，后者是IEEE的无线局域网协议。**IEEE 802.1x协议能够在IEEE 802系列局域网协议的基础上，提供一种对连接到局域网的用户进行认证和授权的手段，达到接受合法用户接入，保护网络安全的目的。**

目前WPA和WPA2都使用了IEEE 802.1x作为认证手段。

## 历年试题

●(2003年上) A向B发送消息P，并使用公钥体制进行数字签名。设E表示公钥，D表示私钥，则B要保留的证据是 (31)。基于数论原理的RSA算法的安全性建立在(32) 的基础上。Kerberos是MIT为校园网设计的身份认证系统，该系统利用智能卡产生 (33) 密钥，可以防止窃听者捕获认证信息。为了防止会话劫持，Kerberos提供了 (34) 机制，另外报文中还加入了 (35) ，用于防止重发攻击(replay attack)。

(31)A．EA(P) B．EB(P) C．DA(P) D．DB(P)

(32)A．大数难以分解因子 B．大数容易分解因子C．容易获得公钥 D．私钥容易保密

(33)A．私有 B.加密 C．一次性 D．会话

(34)A．连续加密 B．报文认证 C．数字签名 D．密钥分发

(35)A．伪随机数 B．时间标记 C．私有密钥 D．数字签名

●(2004年下)电子商务交易必须具备不可抵赖性，目的在于防止(19)

（19）A.一个实体假装成另一个实体 B.参与此交易的一方否认曾经发生过此次交易

C.他人对数据进行非授权的修改、破坏 D.信息从被监视的通信过程中泄漏出去

●(2005年上)HTTPS 是一种安全的HTTP 协议，它使用 (53)来保证信息安全，使用 (54)来发送和接受报文。

（53）A．IPSec B．SSL C．SET D．SSH

（54）A．TCP 的443 端口　 B．UDP 的443 端口 C．TCP 的80 端口 D．UDP 的80 端口

●(2005年上)Windows 2000 有两种认证协议，即Kerberos 和PKI，下面有关这两种认证协议的描述中，正确的是(56) 。在使用Kerberos 认证时，首先向密匙分发中心发送初始票据 (57) ，来请求一个会话票据，以便获取服务器提供的服务。

（56）A．Kerberos 和PKI都是对称密钥 B．Kerberos 和PKI 都是非对称密钥

C．Kerberos 是对称密钥，而PKI 是非对称密钥 D．Kerberos 是非对称密钥，而PKI 是对称密钥

（57）A．RSA　 B．TGT　　C．DES　　D．LSA

●(2006年上)下面语句中，正确地描述了RADIUS 协议的是(24)。

(24)A. 如果需要对用户的访问请求进行提问(Challenge)，则网络访问服务器(NAS)对用户密码进行加密，并发送给RADIUS 认证服务器

B. 网络访问服务器(NAS)与RADIUS 认证服务器之间通过UDP 数据报交换请求/响应信息

C. 在这种C/S 协议中，服务器端是网络访问服务器(NAS)，客户端是RADIUS 认证服务器

D. 通过RADIUS 协议可以识别非法的用户，并记录闯入者的日期和时间

●(2007年上)采用Kerberos系统进行认证时，可以在报文中加入（44）防止重放攻击。

（44）A.会话密钥 B.时间戳 C.用户ID D.私有密钥

●(2007年下)安全电子邮件协议PGP不支持（40） 。

（40）A．确认发送者的身份 B．确认电子邮件未被修改 C．防止非授权者阅读电子邮件D．压缩电子邮件大小

●(2008年上)某银行为用户提供网上服务，允许用户通过浏览器管理自己的银行账户信息。为保障通信的安全性，该Web服务器可选的协议是(9)。

(9)A.POP B.SNMP C.HTTP D.HTTPS

●(2008年下)下列安全协议中， （47） 能保证交易双方无法抵赖。

（47）A．SET B.HTTPS C.PGP D.MOSS

●(2009年下)在Kerberos系统中，使用一次性密钥和（41）来防止重放攻击。

（41）A．时间戳 B．数字签名 C．序列号 D．数字证书

●(2009年下)SSL协议使用的默认端口是 （48） 。

（48）A．80 B．445 C．8080 D．443

●(2010年上)HTTPS采用（39）协议实现安全网站访问。

（39）A．SSL B．IPSec C．PGP D．SET

●(2011年下)以下安全协议中，用来实现安全电子邮件的协议是 （43） 。

（43）A. IPSec B. L2TP C. PGP D. PPTP

●(2012年上)支持安全WEB服务的协议是（43）。

(43)A．HTTPS B．WINS C．SOAP D．HTTP

●(2012年上)安全电子邮件使用（68）协议。

(68)A．PGP B．HTTPS C．MIME D．DES

●(2011年上)HTTPS的安全机制工作在 （48），而S-HTTP的安全机制工作在 （49）。

（48）A.网络层 B.传输层C.应用层D.物理层

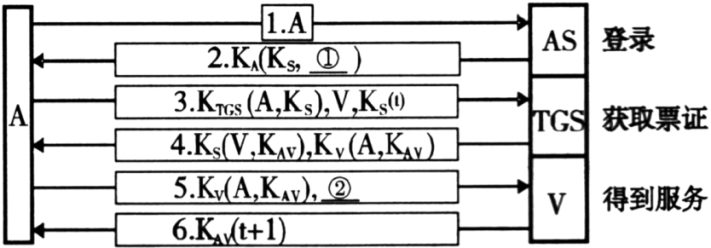
（49）A.网络层 B.传输层C.应用层 D.物理层

●(2011年上)在Kerberos认证系统中，用户首先向（46）申请初始票据，然后从（47）获得会话密钥。

（46）A.域名服务器DNS B.认证服务器AS C.票据授予服务器TGS D.认证中心CA

（47）A.域名服务器DNS B.认证服务器AS C.票据授予服务器TGS D.认证中心CA

●(2011年下)Kerberos由认证服务器（AS）和票证授予服务器（TGS）两部分组成，当用户A通过Kerberos向服务器V请求服务时，认证过程如下图所示，图中①处为 （44） ，②处为 （45） 。



（44）A. KTGS(A,KS) B.KS(V,KAV) C. KV(A,KAV) D. KS(t)

（45）A. KAV(t+1) B. KS(t+1) C. KS(t) D. KAV(t)

●(2013年上)（43)是支持电子邮件加密服务的协议。

(43) A.PGP B.PKI C.SET D.Kerberos

●(2014年上)与HTTP1.0相比，HTTP1.1的优点不包括（30）。

(30)A.减少了RTTs数量 B.支持持久连接 C.减少了TCP慢启动次数 D.提高了安全性

解析：

* HTTP/1.0的每次请求和响应都需要建立一个单独的连接，每次连接只是传输一个对象，严重影响客户机和服务器的性能。HTTP/1.1支持持久连接，在一个TCP连接上可以传送多个HTTP请求和响应，减少了建立和关闭连接的消耗和延迟。
* HTTP/1.1通过增加更多的请求头和响应头来改进和扩充HTTP 1.0的功能。在HTTP 1.1中增加Host请求头字段后，实现了在一台WEB服务器上可以在同一个IP地址和端口号上使用不同的主机名来创建多个虚拟WEB站点。
* HTTP/1.1的持续连接，也需要增加新的请求头来帮助实现，例如，Connection请求头的值为Keep-Alive时，客户端通知服务器返回本次请求结果后保持连接；Connection请求头的值为close时，客户端通知服务器返回本次请求结果后关闭连接。
* HTTP/1.1还有身份认证机制，许多Web站点要求用户提供一个用户名—口令对才能访问存放在其服务器中的文档，这种要求称为身份认证(authentication)。HTTP提供特殊的状态码和头部来帮助Web站点执行身份认证。
* HTTP/1.1支持文件断点续传，而HTTP1.0每次传送文件都是从文件头开始，即0字节处开始。

●(2014年下，2017年上)PGP(Pretty Good Privacy)是一种电子邮件加密软件包，它提供数据加密和数字签名两种服务，采用 (42) 进行身份认证，使用 (43) (128位密钥)进行数据加密，使用 (44) 进行数据完整性验证。

(42)A.RSA公钥证书 B.RSA私钥证书 C.Kerboros证书 D.DES私钥证书

(43)A.IDEA B.RSA C.DES D.Diffie-Hellman

(44)A.HASH B.MD5 C.三重DES D.SHA-1

●(2014年下)以下关于S-HTTP的描述中，正确的是 (45) 。

(45)A.S-HTTP是一种面向报文的安全通信协议，使用TCP 443端口 B.S-HTTP所使用的语法和报文格式与HTTP相同

C.S-HTTP也可以写为HTTPS D.S-HTTP的安全基础并非SSL

●(2015年上)提供电子邮件安全服务的协议是 (41) 。

(41)A.PGP B.SET C.SHTTP D.Kerberos

●(2015年上)Kerberos是一种 (44) 。

(44)A.加密算法 B.签名算法 C.认证服务 D.病毒

●(2015年上)IEEE802.1x是一种基于 (51) 认证协议。

(51)A.用户ID B.报文 C.MAC地址 D.SSID

●(2015年下)下列（44）不能提供应用层安全。

(44)A.S-HTTP B.PGP C.MIME D.SET

●(2018年上)网络管理员通过命令行方式对路由器进行管理，需要确保ID、口令和会话内容的保密性，应采取的访问方式是(7）。

(7)A.控制台 B.AUX C.TELNET D.SSH

●(2019年上)下述协议中与安全电子邮箱服务无关的是 (8) 。

(8)A.SSL B.HTTPS C.MIME D.PGP

# 网络体系结构

**在进行关于网络安全设计时，所要遵循的设计原则为：**

#### 要充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件；

#### 要强调安全防护、监测和应急恢复。要求在网络发生被攻击的情祝下，必须尽可能快地恢复网络信息中心的服务，减少损失；

#### 考虑安全问题解决方案时一定要考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合；

#### 网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提。

图 11.1是对在TCP/IP参考模型各层使用的安全协议的总结：



图 11.1 TCP/IP参考模型各层使用的安全协议

## 历年试题

●(2006年上)网络安全设计是保证网络安全运行的基础，网络安全设计有其基本的设计原则，以下关于网络安全设计原则的描述，错误的是 (60) 。

(60)A．网络安全的“木桶原则”强调对信息均衡、全面地进行保护 B．良好的等级划分，是实现网络安全的保障

C．网络安全系统设计应独立进行，不需要考虑网络结构 D．网络安全系统应该以不影响系统正常运行为前提

●(2009年上)以下关于网络安全设计原则的说法，错误的是(39)。

（39）A.充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件。

B．强调安全防护、监测和应急恢复。要求在网络发生被攻击的情祝下，必须尽可能快地恢复网络信息中心的服务，减少损失。

C．考虑安全问题解决方案时无需考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合

D．网络安全应以不能影响系统的正常运行和用户合法用户的操作活动为前提。

●(2015年下)为防止WWW服务器与浏览器之间传输的信息被窃听，可以采取(47)来防止该事件的发生。

(47)A.禁止浏览器运行ActiveX控件 B．索取WWW服务器的CA证书

C．将WWW服务器地址放入浏览器的可信站点区域 D．使用SSL对传输的信息进行加密

# 防火墙

防火墙是一种网络访问控制软件或设备，是置于不同网络安全域之间的一系列部件的组合，是不同网络安全域间通信的唯一通道，能根据企业有关的安全策略控制（允许、拒绝、监视、记录）进出网络的访问行为。

## 防火墙的基本类型

### 包过滤防火墙

**包过滤防火墙也称为访问控制列表，它是根据已经定义好的过滤规则来审查每个数据包，并确定该数据包是否与过滤规则匹配，从而决定数据包是否能通过。**

**过滤：源IP，源port，目标IP，目标port,网络协议**

包过滤防火墙工作在网际层和传输层之间，其优点是：可以与现有的路由器集成，也可以用独立的包过滤软件来实现，而且数据包过滤对用户来说是透明的，成本低、速度快、效率高。

缺点：

* 包过滤技术的主要依据是包含在IP报头中的各种信息，可是IP包中信息的可靠性没有保证，IP源地址可以伪造，通过内部合谋，入侵者轻易就可以绕过防火墙；
* 并非所有的服务都与静态端口绑定，包过滤只能够过滤IP地址，所以它不能识别相同IP地址下不同的用户，从而不具备身份认证的功能；
* 工作在网络层，不能检测那些对高层进行的攻击；
* 如果为了提高安全性而使用很复杂的过滤规则，那么效率会大大降低；
* 对每一个数据包单独处理，不具备防御DoS攻击和DDos攻击的能力。

### 状态检测防火墙

状态检测防火墙是一种**动态包过滤防火墙**，也称为自适应防火墙，它在**基本包过滤防火墙的基础上增加了状态检测功能**。

优点是：

* 具备包过滤防火墙的一切优点；
* 能够灵活地动态地生成过滤规则；
* 具备较好的DoS攻击和DDoS攻击防御能力；
* 与应用代理防火墙相比，执行效率较高，具有较好的可伸缩性和易扩展性，应用范围广。
* 缺点：
* 不能对应用层数据进行控制；
* 不能记录高层次的日志。

### 应用代理防火墙

应用代理防火墙工作在应用层，针对专门的应用层协议制定数据过滤和转发规则。其核心技术是代理服务器技术。

优点：

* 可实现身份认证；
* 可进行内容过滤；
* 可记录非常详尽的应用层日志记录。

缺点：

* 工作效率低
* 对不同的应用层服务都可能需要定制不同的应用代理防火墙软件，缺乏灵活性，不易扩展。

## 典型防火墙拓扑结构



图 12.1 防火墙部署



图 12.2典型的防火墙部署拓扑结构

如图 12.1所示，服务器放置于防火墙的DMZ区域（Demilitarized Zone，隔离区域）；用户联网区放置于防火墙的Inside区域，通过防火墙的安全防护策略，外部网络只能访问DMZ区域的相应服务，不能直接进入Inside区域。防火墙连接路由器的一端称为Outside端，其安全度为0，Inside区域认为安全度为100，而DMZ区域由于外网用户可进入此区访问相应的服务，故认为安全度在Inside和Outside之间，一般可设置为50。

一个典型的防火墙部署拓扑结构如图 12.2所示。

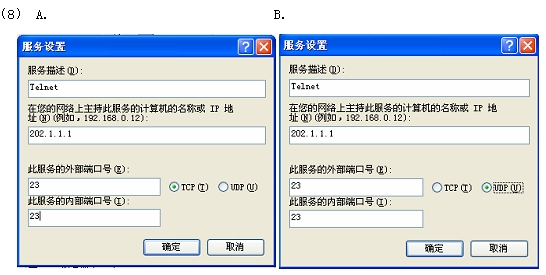
## 历年试题

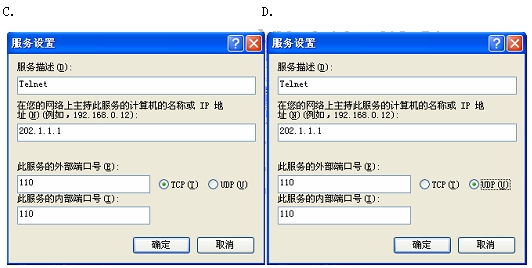
●(2007年上)包过滤防火墙通过（45）来确定数据包是否能通过。

（45）A.路由表 B.ARP表 C.NAT表 D.过滤规则

●(2008年上)如果希望别的计算机不能通过ping命令测试[服务器](http://www.educity.cn/incsearch/search.asp?key=%B7%FE%CE%F1%C6%F7)的连通情况，可以(7)。如果希望通过默认的Telnet端口连接服务器，则下面对[防火墙](http://www.educity.cn/incsearch/search.asp?key=%B7%C0%BB%F0%C7%BD)配置正确的是 (8) 。

(7)A.删除服务器中的ping.exe文件 B.删除服务器中的cmd.exe文件 C.关闭服务器中ICMP 端口 D.关闭服务器中的Net Logon服务





●(2009年上)包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括 （48） 。

（48）Ａ.源地址　　B.目的地址　　　Ｃ.协议　　　Ｄ.有效载荷

●(2009年下)包过滤防火墙对数据包的过滤依据不包括（8）。

（8）A. 源 IP 地址 B. 源端口号 C. MAC 地址 D. 目的 IP 地址

●(2010年下)下列选项中，防范网络监听最有效的方法是（9） 。

（9）A.安装防火墙 B.采用无线网络传输 C.数据加密 D.漏洞扫描

●(2014年上)防火墙的工作层次是决定防火墙效率及安全的主要因素，以下叙述中，正确的是 (8) 。

(08)A．防火墙工作层次越低，工作效率越高，安全性越高 B．防火墙工作层次越低，工作效率越低，安全性越低

C．防火墙工作层次越高，工作效率越高，安全性越低 D．防火墙工作层次越高，工作效率越低，安全性越高

●(2014年上)以下关于包过滤防火墙和代理服务防火墙的叙述中，正确的是 (9) 。

(09)A．包过滤技术实现成本较高，所以安全性能高 B．包过滤技术对应用和用户是透明的

C．代理服务技术安全性较高，可以提高网络整体性能 D．代理服务技术只能配置成用户认证后才建立连接

●(2014年下)网络系统中，通常把 (7) 置于DMZ区。

(07)A.网络管理服务器 B.Web服务器 C.入侵检测服务器 D.财务管理服务器

●(2019年上) (7) 防火墙是内部网和外部网的隔离点,它可对应用层的通信数据流进行监控和过滤。

(7)A.包过滤 B.应用级网关 C.数据库 D.WEB

# 病毒防护

计算机病毒是指**编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据影响计算机使用，并能自我复制的一组计算机指令或者程序代码。**

计算机病毒的特性：**传染性、非授权可执行性、隐蔽性、潜伏性、破坏性、可触发性**。

## 病毒的类型

* **寄生虫病毒。**传统的并且仍是最常见的病毒形式。寄生虫病毒将自己附加到可执行文件中，当被感染的程序执行时，找到其他可执行程序文件并感染；
* **存储器驻留病毒。**寄宿在主存中，作为驻留程序的一部分。从那时开始，病毒感染每个执行的程序；
* **引导区病毒。**感染主引导记录或引导记录，并且当系统从包含了病毒的磁盘启动时进行传播；
* **隐形病毒。**病毒的一种形式，明确地设计成能够在反病毒软件检测时隐藏自己；
* **多形病毒。**每次感染时会改变的病毒，使得不可能通过病毒的“签名”来检测。

## 常见的病毒及木马、蠕虫等



图 13.1 常见病毒及木马、蠕虫等

## 历年试题

●(2006年上)DNS 系统对于网络的正常运行是至关重要的，以下措施中不能增强DNS 安全性的是 (40) 。

(40)A. 使用防火墙控制对DNS 的访问 B. 避免DNS 的HINFO 记录被窃取 C. 更改DNS 的端口号 D. 限制区域传输

●(2007年上)感染“熊猫烧香”病毒后的计算机不会出现（9）的情况。

（9）A.执行文件图标变成熊猫烧香 B.用户信息被泄漏 C.系统运行变慢 D.破坏计算机主板

●(2007年上)在网络上流行的“熊猫烧香”病毒属于（46）类型的病毒。

（46）A.目录 B.引导区 C.蠕虫 D.DOS

●(2009年下)在下面4种病毒中，（42）可以远程控制网络中的计算机。

(42)A．worm.Sasser.f B．Win32.CIH C．Trojan.qq3344 D．Macro.Melis

●(2010年上)杀毒软件报告发现病毒Macro.Melissa，由该病毒名称可以推断出病毒类型是（40），这类病毒主要感染目标是（41）。

（40）A.文件型 B.引导型 C．目录型D．宏病毒

（41）A.EXE或COM可执行文件 B.WORD或EXCEL文件 C.DLL系统文 D.磁盘引导区

●(2011年上)下面病毒中，属于蠕虫病毒的是（50）。

（50）A.Worm.Sasser病毒 B.Trojan.QQPSW病毒C.Backdoor.IRCBot病毒 D.Macro.Melissa病毒

●(2011年上)宏病毒一般感染以（8）扩展名的文件。

（8）A.EXE B.COM C.DOC D.DLL

●(2011年下)通过内部发起连接与外部主机建立联系，由外部主机控制并盗取用户信息的恶意代码为（8） 。

（8）A. 特洛伊木马 B. 蠕虫病毒 C. 宏病毒 D. CIH病毒

●(2013年上)近年来，在我国出现的各类病毒中，（34）病毒通过木马形式感染智能手机。

(34)A.欢乐时光 B.熊猫烧香 C.X卧底 D.CIH

●(2014年下) (9) 不是蠕虫病毒。

(9)A.熊猫烧香 B.红色代码 C.冰河 D.爱虫病毒

●(2015年上)宏病毒可以感染后缀为 (43) 的文件。

(43)A.exe B.txt C.pdf D.xls

●(2019年上)计算机病毒的特征不包括 (8) 。

(8) A.传染性 B.触发性 C.隐蔽性 D.自毁性

●(2019年上)震网(Stuxnet)病毒是一种破坏工业基础设施的恶意代码，利用系统漏洞攻击工业控制系统，是一种危害性极大的 （62） 。

（62）A、引导区病毒 B、宏病毒 C、木马病毒 D、蠕虫病毒

# 入侵检测系统

即使有了**防火墙和杀毒软件**，还是不能保证网络的绝对安全。这是因为网络安全是一个复杂的系统工程，单纯的被动防御是难以凑效的，所有必要引入另外的主动防御技术，而**入侵检测系统（Intrusion Detection System，IDS）可作为防火墙之后的第二道安全屏障，对网络活动进行实时的检测。**

美国国防部高级研究计划局(DARPA)提出的公共入侵检测框架(Common Intrusion Detection Framework，CIDF)由4个模块组成，。



图 14.1 入侵检查框架

* 事件产生器(Event generators，E-boxes)。负责数据的采集，并将收集到的原始数据转换为事件，向系统的其他模块提供与事件有关的信息。
* 事件分析器(Event Analyzers，A-boxes)。接收事件信息并对其进行分析，判断是否为入侵行为或异常现象。采用的分析方法有模式匹配、数据完整性分析和统计分析方法。
* 事件数据库(Event DataBase，D-boxes)。存放有关事件的各种中间结果和最终数据的地方，可以是面向对象的数据库，也可以是一个文本文件。
* 响应单元(Response units，R-boxes)。根据报警信息作出各种反应，强烈的反应就是断开连接、改变文件属性等，简单的反应就是发出系统提示，引起操作人员注意。

## IDS的入侵检测分析方法

* 异常检测：定义正常行为，与之不同为入侵行为；
* 滥用检测(基于知识的检测)：输入入侵行为特征，与之匹配则为入侵，其他均为正常行为。

## 入侵检测系统的部署

入侵检测系统是一个监听设备，无须跨接在任何链路上，它不产生任何网络流量便可以工作。因此，对IDS部署的唯一要求是**应当挂接在所关注流量必须流经的链路上**。在这里，“所关注流量指的是来自高危网络区域的访问流量以及需要统计、监视的网络报文。目前的网络都是变换式的拓扑结构，因此一般选择在尽可能靠近攻击源，或者尽可能接近受保护资源的地方，这些位置通常是：

* 服务器区域的交换机上；
* Internet接入路由器的第一个交换机上；
* 重点保护网段的局域网交换机上。

典型的入侵检测系统的部署方式如图 14.2所示。



图 14.2典型的入侵检测系统的部署

根据入侵检测系统的信息来源，可分为基于主机的IDS、基于网络的IDS以及基于分布式的IDS，对这几种IDS的特点分析如下。

主机入侵检测系统（HIDS）

这是针对主机或服务器的入侵行为进行检测和相应的系统；它的优点是性价比较高，检测更加细致，误报率比较低，适用于加密和交换的环境，对网络流量不敏感，而且还可以确定攻击是否成功。缺点是：首先，由于HIDS依赖丁主机内建的日志与监控能力，而主机审计信息易于受到攻击，入侵者甚至可设法逃避审计，所以这种入侵检测系统的可靠性不是很高。其次，HIDS只能对主机的特定用户、特定应用程序和日志文件进行检测，所能检测到的攻击类型受到一定的限制。最后，HIDS的运行或多或少地影响主机的性能，全面部署HIDS的成本也比较大。

网络入侵检测系统（NIDS）

这是针对整个网络的入侵检测系统，包括对网络中的所有主机和交换设备进行入侵行为的监测和响应，其特点是利用工作在混杂模式下的网卡来实时监听整个网段上的通信业务。

优点是隐蔽性好，不影响网络业务流量。由于实时检测和响应，攻击者不容易转移证据，会留下蛛丝马迹，并能够检测出来获成功的攻击企图。

它的缺点是只检测直接连接的网络段的通信，不能检测到不同网段的数据包，在交换式以太网环境中会出现检测范围的局限性。另外，NIDS在实时监控环境下很难实现列复杂的、需要大量计算与分析时间的攻击的检测。例如，网络中的有些会话过程是经过加密的，这对于实时工作的NIDS也难于处理。

分布式入侵检测系统（DIDS）

由分布在网络各个部分的多个协同工作的部件组成，分别完成数据采集、数据分析和入侵响应等功能，并通过中央控制部件进行入侵检测数据的汇总和数据的维护，协调各个部件的工作。这种系统比较庞大，成本较高。

## 历年试题部分

●(2006年下)关于网络安全，以下说法中正确的是（32）。

（32）A.使用无线传输可以防御网络监听 B.木马是一种蠕虫病毒

C.使用防火墙可以有效地防御病毒 D.冲击波病毒利用 Windows 的 RPC 漏洞进行传播

解析：

RPC(Remote Procedure Call):远程过程调用

●(2006年上)(37) 不属于将入侵检测系统部署在DMZ 中的优点。

(37)A. 可以查看受保护区域主机被攻击的状态B. 可以检测防火墙系统的策略配置是否合理

C. 可以检测DMZ 被黑客攻击的重点 D. 可以审计来自Internet 上对受保护网络的攻击类型

●(2009年上)安全审计是保障计算机系统安全的重要手段，其作用不包括（67）。

（67）A．重现入侵者的操作过程 B．发现计算机系统的滥用情况

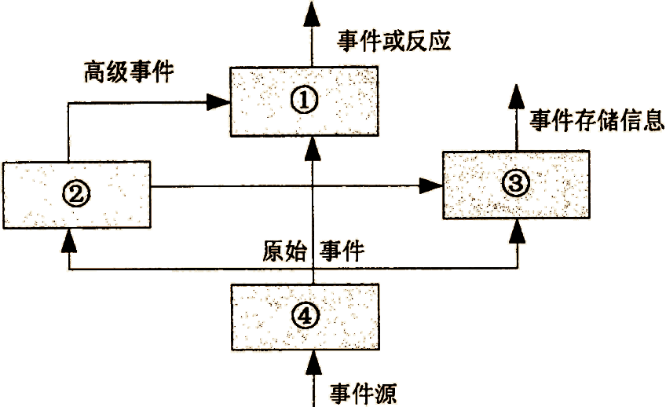
C．根据系统运行的日志，发现潜在的安全漏洞 D．保证可信计算机系统内部信息不外泄

●(2010年上)某局域网访问internet 速度很慢，经检测发现局域网内有大量的广播包，采用（49）方法不可能有效的解决该网络问题。

（49）A．在局域网内查杀ARP病毒和蠕虫病毒　B．检查局域网内交换机端口和主机网卡是否有故障

　　　C．检查局域网内是否有环路出现 　　　D．提高出口带宽速度

●(2013年上)下图为DARPA提出的公共入侵检测框架示意图，该系统由4个模块组成。其中模块①～④对应的正确名称为（45) 。



(45) A.事件产生器、事件数据库、事件分析器、响应单元 B.事件分析器、事件产生器、响应单元、事件数据库

C.事件数据库、响应单元、事件产生器、事件分析器 D.响应单元、事件分析器、事件数据库、事件产生器

●(2014年上)在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法中不包括 (45) 。

(45)A．模式匹配 B．密文分析 C．数据完整性分析 D．统计分析

●(2014年上)在Windows Server 2003环境中有本地用户和域用户两种用户。其中本地用户信息存储在 (46) 。

(46)A．本地计算机的SAM数据库 B．本地计算机的活动目录 C．域控制器的活动目录 D．域控制器的SAM数据库

解析：

在操作系统中，计算机的账户是用户登录系统的钥匙，当用户想要进入一台计算机的操作系统对计算机进行操作和管理的时候，必须有一个相应的账户才可以，在Windows环境下的计算机账户从计算机的管理模式来分主要分为本地用户账户和域账户两种，这两种账户有以下特点和区别：

1.本地用户账户是在工作组环境上或是域的成员机登录本地机器所使用的账户名和密码，而域账户是在域的管理模式下域上的用户所使用的账户。

2.本地用户账户存储在本地的sam数据库中，而域账户存储在AD（Active Directory）中。

3.使用本地用户账户的时候，用户只能使用该账户登录到本地计算机上,而使用域账户用户可以在整个域环境中所有的计算机上进行登录。

4.本地账户只能在账户所属的计算机上进行管理，每个计算机上的管理员单独管理自己机器上的本地账户，而域账户通过AD用户和计算机管理工具进行统一的管理。本题选择A选项。

●（2015年上）IDS设备的主要作用是 (42) 。

(42)A.用户认证 B.报文认证 C.入侵检测 D.数据加密

●(2015年下)防火墙不具备（45）功能。

(45)A.包过滤 B.查毒 C．记录访问过程 D.代理

●(2017年下)以下关于入侵检测系统的描述中，正确的是 (45) 。

(45)A.实现内外网隔离与访问控制 B.对进出网络的信息进行实时的监测与比对，及时发现攻击行为

C.隐藏内部网络拓扑 D.预防、检测和消除网络病毒

●(2017年下) (65) 不属于入侵检测技术。

(65)A.专家系统 B.模型检测 C.简单匹配 D.漏洞扫描

●(2018年上)在网络安全管理中，加强内防内控可采取的策略有 (10) 。

①控制终端接入数量 ②终端访问授权，防止合法终端越权访问 ③加强终端的安全检查与策略管理

④加强员工上网行为管理与违规审计

(10)A.②③ B.②④ C.①②③④ D.②③④

# 入侵防御系统

## 入侵防御系统与防火墙及IDS区别

随着网络入侵事件的不断增加和黑客攻击水平的不断提高，一方面，局域网络感染病毒、遭受攻击的速度日益加快；另一方面，局域网络受到攻击做出响应的时间却越来越滞后。面对这一矛盾，传统的防火墙或入侵检测技术越来越显得力不从心，由此产生了IPS(Intrusion-preventionsystem，入侵防御系统）。与传统的防火墙提供的访问控制策略以及IDS提供的被动防御不同，IPS是一种主动的、积极的入侵防御系统。它能对入侵活动进行实时的预先检查和对攻击性网络流量进行拦截，而不是在恶意流量传送时或传送后才发出警报。IPS与防火墙和IDS的区别如下：

* IPS与防火墙的比较：传统的防火墙是实施访问控制策略的系统，通过对流经的网络流量进行检查，拦截不符合安全策略的数据报，拒绝明显可疑的网络流量。防火墙只能基于数据包的包头进行检查，不能对数据内容进行检查，因此对很多入侵行为无法防御。IPS的过滤技术与防火墙的包过滤技术不同，它可以做到逐一字节地检查数据报，深入检查数据报中的内容，如果数据内容被分析出存在攻击意图，IPS可以阻止数据报通过。

IPS与IDS的比较：对于入浸行为，IDS只是检测和报警，并不具有真正的防御和阻止攻击的能力。IPS是一种比较主动的防御系统，不仅能检测到入侵行为，还能采取相应的措施进行阻止。IPS是在网络入口进行入侵检测和响应的，能在一些入侵行为造成破坏之前将其阻止，从而提高了网络的安全性。在检测能力方面，IPS是在应用层的内容检测基础上加上主动响应和过滤功能，弥补了传统的防火墙＋IDS方案的不足。

## IPS部署方式

IPS在网络中的部署方式有如下几种：

旁路模式

旁路模式是指设备不在数据转发的链路上，通常是通过接收流量镜像、探测复制报文的方式捕获数据报文，缺点是无法阻止恶意流量比如单包攻击。如果要阻止这样的攻击需要其它设备（路由器、交换机、防火墙）来协助。所以是一种“知而不决”的行为。如图 15.1所示为IPS的旁路连接模式。



图 15.1旁路模式

在图 15.1中，需要将交换机其他端口的数据流量转发到与IPS连接的交换机端口G1/1来以便IPS实现对网络的监听，这要求G1/1工作在镜像端口状态。端口镜像（port Mirroring）功能通过在交换机或路由器上将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口”或“目的端口”，在不严重影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。在企业中用镜像功能，可以很好地对企业内部的网络数据进行监控管理，在网络出故障的时候，可以快速地定位故障。

混杂模式

该模式下，IPS并联在网络中，受监控网段的数据包不流经IPS，通过在交换机上配置SPAN，把流经交换机的流量拷贝给IPS，这相当干传统的IDS设备。混杂模式如图 15.2所示。



图 15.2 混杂模式

在混杂模式下，由于网络流量不经过IPS，不会增加网络的滞后时间，但IPS对攻击的响应能力有限，不能很好地抵御各种网络攻击和网络蠕虫病毒，因此在该模式下，IPS必须和防火墙联动以有效地遏制攻击。

在线接口模式

在该模式下，IPS串联在网络中，网络流量直接流经IPS设备，IPS会在恶意的流量到达指定的目标之前阻断该流量从而防止目标受到攻击。IPS不仅处理数据包的第3层和第4层信息，还分析数据包的有效载荷从而发现更深层次的攻击，深度审查使IPS可以识别和阻断那些能够穿越传统防火墙的攻击。在线接口模式如图 15.3所示。



图 15.3在线接口模式

在线接口模式下，IPS的两个接口被配置为接口对，数据包从接口对中的一个接口进，从另一个接口出。当数据包从接口对中的一个接口进入IPS后，IPS会根据特征库对数据包进行审查以决定将数据包转发至接口对中的另一个接口或是直接丢弃。

在线VLAN对模式

IPS的一个物理接口可以关联多个VLAN对，交换机和IPS间的链路是802.10 trunk链路。IPS用物理接口的子接口来对一对VLAN的流量进行检测。



图 15.4 在线Vlan对模式

如图 15.4所示，VLANIO到VLAN20之间的流最经过IPS，在该模式下，一个子接口关联一对VLAN。一个物理接口支持255个子接口，因此，该模式的优点是一个物理接口可以关联255个VLAN对，减少了对物理接口的需求。

VLAN组模式

IPS的物理接口被划分成VLAN组子接口，每个子接口可以关联一组VLAN，且在该模式下分析引擎支持多个虚拟的传感器（Virtual Sensor，VS），每个虚拟的传感器可以监控一个或多个VLAN组子接口，这种特性可以实现在同一个传感器上配置不同的策略。