系统安全性分析与设计

系统安全体系结构

- 作为全方位的、整体的系统安全防范体系也是分层次的，不同层次反映了不同的安全问题，根据网络的应用现状情况和结构，可以将安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理。
- （1）物理环境的安全性。物理层的安全包括通信线路、物理设备和机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件和传输介质）、软硬件设备的安全性（替换设备、拆卸设备、增加设备）、设备的备份、防灾害能力、防干扰能力、设备的运行环境（温度、湿度、烟尘）和不间断电源保障等。

- （2）操作系统的安全性。系统层的安全问题来自计算机网络内使用的操作系统的安全，例如，Windows Server和UNIX等。主要表现在3个方面，一是由操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。
- （3）网络的安全性。网络层的安全问题主要体现在计算机网络方面，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。

- （4）应用的安全性。应用层的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括Web服务、电子邮件系统和DNS等。此外，还包括病毒对系统的威胁。
- （5）管理的安全性。安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个计算机网络的安全，严格的安全管理制度、明确的部门安全职责划分与合理的人员角色配置，都可以在很大程度上降低其他层次的安全漏洞。

典型真题

- ● 网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。 其中，数据库容灾属于（ ）。
- A．物理线路安全和网络安全　　B.应用安全和网络安全
- C.系统安全和网络安全　　D.系统安全和应用安全

- 试题分析
- 数据库属于应用系统，又与操作系统相关，因此属于系统安全和应用安全。
- 参考答案：（70）D

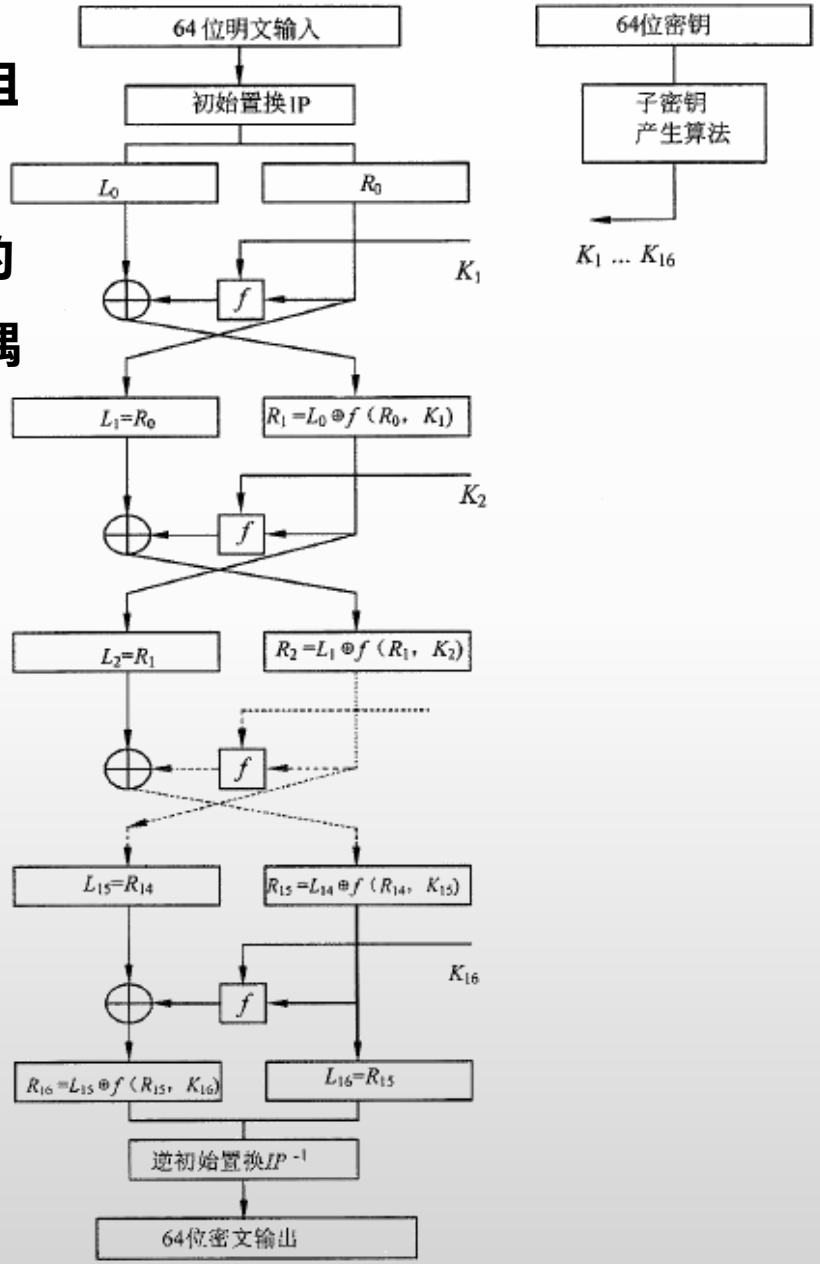
数据加密技术

- 1．对称加密算法

- 对称加密算法也称为私钥加密算法，是指加密密钥和解密密钥相同，或者虽然不同，但从其中的任意一个可以很容易地推导出另一个。其优点是具有很高的保密强度，但密钥的传输需要经过安全可靠的途径。对称加密算法有两种基本类型，分别是分组密码和序列密码。分组密码是在明文分组和密文分组上进行运算，序列密码是对明文和密文数据流按位或字节进行运算。

- 常见的对称加密算法包括瑞士的国际数据加密算法（International Data Encryption Algorithm, IDEA）和美国的数据加密标准（Date Encryption Standard, DES）。

- DES是一种迭代的分组密码，明文和密文都是64位，使用一个56位的密钥以及附加的8位奇偶校验位。



- 攻击DES的主要技术是穷举法，由于DES的密钥长度较短，为了提高安全性，就出现了使用112位密钥对数据进行三次加密的算法（3DES），即用两个56位的密钥K1和K2，发送方用K1加密，K2解密，再使用K1加密；接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。
- IDEA是在DES的基础上发展起来的，类似于3DES。IDEA的明文和密文都是64位，密钥长度为128位。

- **2．非对称加密算法**

- **非对称加密算法也称为公钥加密算法，是指加密密钥和解密密钥完全不同，其中一个为公钥，另一个为私钥，并且不可能从任何一个推导出另一个。它的优点在于可以适应开放性的使用环境，可以实现数字签名与验证。**

- **最常见的非对称加密算法是RSA，该算法的名字以发明者的名字命名：Ron Rivest, AdiShamir和Leonard Adleman。RSA算法的密钥长度为512位。RSA算法的保密性取决于数学上将一个数分解为两个素数的问题的难度，根据已有的数学方法，其计算量极大，破解很难。但是加密/解密时要进行大指数模运算，因此加密/解密速度很慢，主要用在数字签名中。**

典型真题

- DES 是一种( )，其密钥长度为 56 位，3DES 是利用 DES 的加密方式，对明文进行 3 次 加密，以提高加密强度，其密钥长度是 ( ) 位。

（6）A.共享密钥 B. 公开密钥C. 报文摘要 D.访问控制

（7）A.56　　B.112　　C.128　　D.168

试题分析

DES加密是一种对称加密算法，加密与解密秘钥相同。由于DES的密钥长度较短，为了提高安全性，就出现了使用112位密钥对数据进行三次加密的算法（3DES），即用两个56位的密钥K1和K2，发送方用K1加密，K2解密，再使用K1加密；接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

参考答案：（6）A　　（7）B

认证技术

认证（authentication）又称为鉴别或确认，它是证实某事物是否名符其实或是否有效的一个过程。认证和加密的区别在于，加密用于确保数据的保密性，阻止对手的被动攻击，例如，截取和窃听等；而认证用于确保数据发送者和接收者的真实性和报文的完整性，阻止对手的主动攻击，例如，冒充、篡改和重放等。认证往往是许多应用系统中安全保护的第一道设防，因而极为重要。

- **1．数字签名**

- **数字签名是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人（例如，接收者）进行伪造。基于对称加密算法和非对称加密算法都可以获得数字签名，但目前主要是使用基于非对称加密算法的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法有RSA、ElGamal、Fiat-Shamir、Des/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等，特殊数字签名算法有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名和具有消息恢复功能的签名等，它与具体应用环境密切相关。数字签名的主要功能是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。**

- 不管使用哪种算法，数字签名必须保证以下三点：
- （1）接收者能够核实发送者对数据的签名，这个过程称为鉴别。
- （2）发送者事后不能抵赖对数据的签名，这称为不可否认。
- （3）接收者不能伪造对数据的签名，这称为数据的完整性。

- **2．杂凑算法**

- **杂凑算法是主要的数字签名算法，它是利用散列（Hash）函数（哈希函数、杂凑函数）进行数据的加密。单向Hash函数提供了这样一种计算过程：输入一个长度不固定的字符串，返回一串定长的字符串，这个返回的字符串称为消息摘要（Message Digest, MD），也称为Hash值或散列值。Hash函数主要可以解决以下两个问题，首先，在某一特定的时间内，无法查找经Hash操作后生成特定Hash值的原消息；其次，无法查找两个经Hash操作后生成相同Hash值的不同消息。这样，在数字签名中就可以解决验证签名、用户身份验证和不可抵赖性的问题。**

- （1）消息摘要算法。消息摘要算法（Message Digest algorithm 5, MD5）用于确保信息传输完整一致，经MD2、MD3和MD4发展而来。它的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式，即将一个任意长度的字节串变换成一个定长的大数）。不管是MD2、MD4还是MD5，它们都需要获得一个随机长度的信息并产生一个128位的消息摘要。MD5以512位分组来处理输入的信息，且每个分组又被划分为16个32位子分组，经过一系列的处理后，算法的输出由4个32位分组组成，将这4个32位分组级联后，将生成一个128位的散列值。

- （2）安全散列算法。安全散列算法（Secure Hash Algorithm, SHA）能计算出一个数字信息所对应的长度固定的字符串（消息摘要），它对长度不超过264位的消息产生160位的消息摘要。这些算法之所以称作“安全”，是基于以下两点，第一，由消息摘要反推原输入信息，从计算理论上来说是很困难的；第二，想要找到两组不同的信息对应到相同的消息摘要，从计算理论上来说也是很困难的；任何对输入信息的变动，都有很高的概率导致其产生的消息摘要不同。

- **3．数字证书**

- **数字证书又称为数字标识，是由认证中心（Certificate Authority, CA）签发的对用户的公钥的认证。数字证书的内容应包括CA的信息、用户信息、用户公钥、CA签发时间和有效期等。目前，国际上对证书的格式和认证方法遵从X.509体系标准。**

- **4．身份认证**

- **用户的身份认证是许多应用系统的第一道防线，其目的在于识别用户的合法性，从而阻止非法用户访问系统。身份识别对确保系统和数据的安全保密是极其重要的，目前，计算机网络系统中常用的身份认证方式主要有以下几种：**

- **（1）口令认证。**

- **（2）动态口令认证。**

- **（3）生物特征识别。**

典型真题

- 要对消息明文进行加密传送，当前通常使用的加密算法是（7）。

（7） A．RSA B．SHA-1

C．MD5 D．RC5

试题分析

RSA是目前最有影响力和最常用的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准。
RSA由于效率问题，一般不直接用于明文加密。

SHA-1与MD5属于信息摘要算法，不能用来加密数据。

RC5是一种对称密码算法，它面向字结构，便于软件和硬件的实现，适用于不同字长的微处理器。

参考答案：（7）D

密钥管理体制

要的密钥管理体制有三种，分别是适用于封闭网、以传统的密钥管理中心为代表的KMI（Key Management Infrastructure，密钥管理基础设施）机制，适用于开放网的PKI（Public Key Infrastructure，公钥基础设施）机制和适用于规模化专用网的SPK（Seeded public-Key，种子化公钥）机制。

通信与网络安全技术

1、防火墙（firewall）

防火墙一般具有以下几个功能：

（1）访问控制功能。这是防火墙最基本也是最重要的功能，通过禁止或允许特定用户访问特定的资源，保护内部网络的资源和数据。需要禁止非授权的访问，防火墙需要识别哪个用户可以访问何种资源，包括服务控制、方向控制、用户控制和行为控制等功能。

（2）内容控制功能。根据数据内容进行控制，例如，防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息，也可以限制外部访问，使它们只能访问本地Web服务器中一部分信息。

（3）全面的日志功能。防火墙需要完整地记录网络访问情况，包括内、外网进出的访问，以检查网络访问情况。一旦网络发生了入侵或者遭到了破坏，就可以对日志进行审计和查询。

（4）集中管理功能。在一个安全体系中，防火墙可能不止一台，因此，防火墙应该是易于集中管理的。

（5）自身的安全和可用性。防火墙要保证自身的安全，不被非法侵入，保证正常的工作。如果防火墙被侵入，安全策略被修改，这样，内部网络就变得不安全。同时，防火墙也要保证可用性，否则网络就会中断，网络连接就会失去意义。

另外，防火墙还应带有如下的附加功能：

（1）流量控制。针对不同的用户限制不同的流量，可以合理使用带宽资源。

（2）网络地址转换（Network Address Translation, NAT）。NAT是通过修改数据包的源地址（端口）或者目的地址（端口）来达到节省IP地址资源，隐藏内部IP地址功能的一种技术。

（3）VPN（Virtual Private Network，虚拟专用网）。只利用数据封装和加密技术，使本来只能在私有网络上传送的数据能够通过公共网络进行传输，使系统费用大大降低。

一般可以分为包过滤型防火墙、电路级网关型防火墙、应用网关型防火墙、代理服务型防火墙、状态检测型防火墙和自适应代理型防火墙。

（1）包过滤型防火墙。包过滤型防火墙是在网络层对数据包进行分析、选择，选择的依据是系统内设置的过滤规则（访问控制表）。通过检查每个数据包的源地址、目的地址、端口和协议状态等因素，确定是否允许该数据包通过。包过滤型防火墙的优点是逻辑简单、成本低，易于安装和使用，网络性能和透明性好，通常安装在路由器上。其缺点是很难准确地设置包过滤器，缺乏用户级的授权；包过滤判别的条件位于数据包的头部，由于IPv4的不安全性，很可能被假冒或窃取；是基于网络层的安全技术，不能检测通过高层协议而实施的攻击。

（2）电路级网关型防火墙。电路级网关型防火墙起着一定的代理服务作用，监视两台计算机建立连接时的握手信息，判断该会话请求是否合法。一旦会话连接有效后，该网关仅复制和传递数据。电路级网关型防火墙在IP层代理各种高层会话，具有隐藏内部网络信息的能力，且透明性高。但由于其对会话建立后所传输的具体内容不再作进一步的分析，因此安全性低。

（3）应用网关型防火墙。应用网关型防火墙是在应用层上实现协议过滤和转发功能，针对特别的网络应用协议制定数据过滤规则。应用网关通常安装在专用工作站系统上，由于它工作于应用层，因此具有高层应用数据或协议的理解能力，可以动态地修改过滤规则，提供记录和统计信息。应用网关型防火墙和包过滤型防火墙有一个共同特点，就是它们仅依靠特定的逻辑来判断是否允许数据包通过，一旦符合条件，则防火墙内外的计算机系统建立直接联系，防火墙外部网络能直接了解内部网络结构和运行状态，这大大增加了实施非法访问攻击的机会。

（4）代理服务型防火墙。代理服务器接收客户请求后，会检查并验证其合法性，如合法，它将作为一台客户机向真正的服务器发出请求并取回所需信息，最后再转发给客户。代理服务型防火墙将内部系统与外界完全隔离开来，从外面只看到代理服务器，而看不到任何内部资源，而且代理服务器只允许被代理的服务通过。代理服务安全性高，还可以过滤协议，通常认为是最安全的防火墙技术。其不足主要是不能完全透明地支持各种服务和应用，而且会消耗大量的CPU资源，导致系统的低性能。

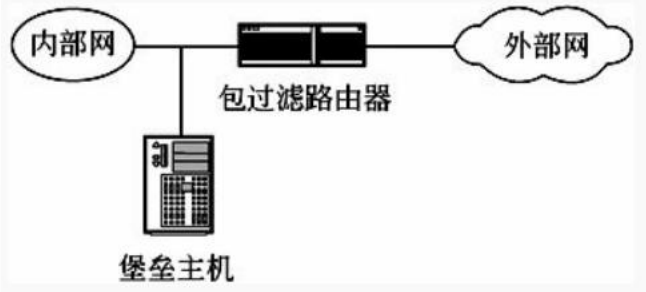
（5）状态检测型防火墙。状态检测型防火墙动态记录和维护各个连接的协议状态，并在网络层对通信的各个层次进行分析与检测，以决定是否允许通过防火墙。因此，状态检测型防火墙兼备了较高的效率和安全性，可以支持多种网络协议和应用，且可以方便地扩展实现对各种非标准服务的支持。

（6）自适应代理型防火墙。自适应代理型防火墙可以根据用户定义的安全策略，动态适应传送中的分组流量。如果安全要求较高，则最初的安全检查仍在应用层完成。而一旦代理明确了会话的所有细节，那么其后的数据包就可以直接经过速度快得多的网络层。因此，此类防火墙兼备了代理技术的安全性和状态检测技术的高效率。

从体系结构上看，防火墙可以有多种实现模式，例如，宿主机模式、屏蔽主机模式和屏蔽子网模式等。

（1）双宿/多宿主机模式。双宿/多宿主机模式是一种拥有两个或多个连接到不同网络上的网络接口的防火墙。通常用一台装有两块或多块网卡的堡垒主机做防火墙，两块或多块网卡各自与内部网和外部网相连，一般采用代理服务的办法，必须禁止网络层的路由功能。

（2）屏蔽主机模式。屏蔽主机模式的防火墙由包过滤路由器和堡垒主机组成。



屏蔽主机模式的主要特点是，在防火墙中堡垒主机安装在内部网络上，通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络唯一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。屏蔽主机防火墙实现了网络层和应用层的安全，因此比单独的包过滤或应用网关代理更安全。在这种模式下，过滤路由器是否配置正确是防火墙安全与否的关键，如果路由表遭到破坏，堡垒主机就可能被越过，使内部网完全暴露。

（3）屏蔽子网模式。屏蔽子网模式采用了两个包过滤路由器和一个堡垒主机，在内外网络之间建立一个被隔离的子网，称为非军事区（De-Militarized Zone, DMZ）或周边网（perimeter network）。

屏蔽子网模式特点是，网络管理员将堡垒主机、Web服务器、Mail服务器等公用服务器放在DMZ中。内部网络和外部网络均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。在这一配置中，即使堡垒主机被入侵者控制，内部网仍能受到内部包过滤路由器的保护。多个堡垒主机运行各种代理服务，可以更有效地提供服务。

当然，防火墙还可能存在着其他的结构模式，例如，一个堡垒主机和一个DMZ、合并DMZ的内部路由器和外部路由器、使用多个堡垒主机、使用多重宿主机与屏蔽子网等。在实际应用中，需要按照网络环境的要求来构造防火墙。

防火墙的使用也有一定的局限性，列举如下：

（1）为了提高安全性，限制或关闭一些有用但存在安全缺陷的网络服务，给用户带来了使用上的不便。

（2）目前，防火墙对于来自网络内部的攻击还无能为力。作为一种被动的防护手段，防火墙不能阻止Internet不断出现的新的威胁和攻击，不能有效地防范数据驱动式攻击。

（3）防火墙不能防范不经过防火墙的攻击，例如，内部网用户通过串行线路网际协议（Serial Line Internet Protocol, SLIP）或点对点协议（Point to Point Protocol, PPP）直接进入Internet。

（4）防火墙对用户不完全透明，可能带来传输延迟、瓶颈和单点失效等。

（5）防火墙不能完全防止受病毒感染的文件或软件的传输，由于病毒的种类繁多，如果要在防火墙完成对所有病毒代码的检查，防火墙的效率就会降到不能忍受的程度。

安全协议

安全协议主要包括IPSec、SSL、PGP和安全套接字层上的超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer, HTTPS）等。

1．SSL

SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL协议可分为两层： SSL记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。 SSL握手协议（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

2．HTTPS

HTTPS是以安全为目标的HTTP通道，简单地说，HTTPS是HTTP的安全版。SSL极难窃听，对中间人攻击提供一定的合理保护。

HTTPS是一个统一资源定位符（Universal Resource Identifier, URI）语法体系，句法类同HTTP体系，用于安全的HTTP数据传输。HTTPS实际上应用了SSL作为HTTP应用层的子层，HTTPS使用端口443（也可以指定其他TCP端口），而不是像HTTP那样使用端口80来和TCP/IP进行通信。HTTPS和SSL支持使用X.509数字认证，如果需要的话，用户可以确认发送者是谁。也就是说，它的主要作用可以分为两种，一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。

3．PGP

PGP是一个基于RSA的邮件加密软件，可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名，从而使收信人可以确信邮件发送者。PGP的基本原理是，先用对称密钥加密传送的信息，再将该对称加密密钥以接收方的公钥加密，组成数字信封，并将此密钥交给公正的第三方保管；然后，将此数字信封传送给接收方。接收方必须先以自己的私钥将数字信封拆封，以获得对称解密密钥，再以该对称解密密钥解出真正的信息，兼顾了方便与效率。PGP还可用于文件存储的加密。

4．IPSec

IPSec是一个工业标准网络安全协议，为IP网络通信提供透明的安全服务，保护TCP/IP通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。IPSec有两个基本目标，分别是保护IP数据包安全和为抵御网络攻击提供防护措施。IPSec结合密码保护服务、安全协议组和动态密钥管理三者来实现上述两个目标。

IPSec是针对IPv4和IPv6的，其主要特征是可以支持IP级所有流量的加密和/或认证，增强所有分布式应用的安全性。IPSec在IP层提供安全服务，使得系统可以选择所需要的安全协议，确定该服务所用的算法，并提供安全服务所需任何加密密钥。

使用IPSec可以显著地减少或防范以下几种网络攻击：

（1）Sniffer。Sniffer可以读取数据包中的任何信息，对抗Sniffer最有效的方法就是对数据进行加密。IPSec的封装安全有效负载（Encapsulating Security Payload, ESP）协议通过对IP包进行加密来保证数据的私密性。

（2）数据篡改。IPSec用密钥为每个IP包生成一个数字检查和，该密钥为且仅为数据的发送方和接收方共享。对数据包的任何篡改，都会改变检查和，从而可以让接收方得知包在传输过程中遭到了修改。

（3）身份欺骗，盗用口令，应用层攻击。IPSec的身份交换和认证机制不会暴露任何信息，不给攻击者有可乘之机，双向认证在通信双方之间建立信任关系，只有可信赖的系统才能彼此通信。

（4）中间人攻击。IPSec结合双向认证和共享密钥，足以抵御中间人攻击。

（5）拒绝服务攻击。IPSec使用IP包过滤法，依据IP地址范围和协议，甚至特定的协议端口号来决定哪些数据流需要受到保护，哪些数据流可以被允许通过，而哪些需要拦截。

入侵检测技术与入侵防护技术

入侵检测是一种主动保护计算机免受攻击的网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全能力（包括安全审计、监视、攻击识别和响应），提高了系统安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行检测。

入侵检测系统（Intrusion-detection system, IDS）一般有两种分类方法，一种是基于数据源的分类，另一种是基于检测方法的分类。

（1）基于数据源的分类。IDS首先需要解决的问题是数据源，或者说是审计事件发生器。IDS根据其检测数据来源可分为两类，分别是基于主机的IDS和基于网络的IDS。基于主机的IDS必须具备一定的审计功能，并记录相应的安全性日志；基于网络的IDS可以放在防火墙或者网关的后面，以网络嗅探器的形式捕获所有的对内和对外的数据包。

（2）基于检测方法的分类。从检测方法上可以将IDS分为异常检测和误用检测两种类型。异常检测也称为基于行为的检测，首先建立用户的正常使用模式（即知识库），标识出不符合正常模式的行为活动；误用检测也称为基于特征的检测，建立已知攻击的知识库，判别当前行为活动是否符合已知的攻击模式。

入侵防护系统（Intrusion Prevention System, IPS）是一种主动的、积极的入侵防范和阻止系统，它部署在网络的进出口处，当检测到攻击企图后，它会自动地将攻击包丢掉或采取措施将攻击源阻断。IPS的检测功能类似于IDS，但IPS检测到攻击后会采取行动阻止攻击。

访问控制

1．自主访问控制

自主访问控制（Discretionary Access Control, DAC）是借助DAC方法中的访问控制表（Access Control List, ACL）。DAC有一个明显的特点，就是这种控制是自主的，它能够控制主体对客体的直接访问，但不能控制主体对客体的间接访问。虽然这种自主性为用户提供了很大的灵活性，但同时也带来了严重的安全问题。所谓间接访问，就是利用访问的传递性，即A可访问B，B可访问C，于是A可访问C。

2．强制访问控制

MAC的基本思想是，每个主体都有既定的安全属性，每个客体也都有既定的安全属性，主体对客体是否能执行特定的操作取决于两者安全属性之间的关系。在实现上，MAC和DAC通常为每个用户赋予对客体的访问权限规则集，考虑到管理的方便，在这一过程中，还经常将具有相同职能的用户聚为组，然后再为每个组分配许可权。用户自主地将自己所拥有的客体的访问权限授予其他用户的这种做法，其优点是显而易见的，但是，当企业的组织结构或系统的安全需求处于变化的过程中时，就需要进行大量繁琐的授权变动，系统管理员的工作将变得非常繁重，容易发生错误造成一些意想不到的安全漏洞。考虑到上述因素，必然会产生新的机制加以解决。

3．基于角色的访问控制

基于角色的访问控制（Role-Based Access Control, RBAC）技术由于其对角色和层次化管理的引进，特别适用于用户数量庞大、系统功能不断扩展的大型系统。在RBAC中，在用户和访问许可权之间引入了角色的概念，用户与特定的一个或多个角色相联系，角色与一个或多个访问许可权相联系。

与DAC和MAC相比，RBAC具有明显的优越性，RBAC基于策略无关的特性，使它几乎可以描述任何安全策略，甚至DAC和MAC也可以用RBAC来描述。相比较而言，RBAC是实施面向企业的安全策略的一种有效的访问控制方式，具有灵活性、方便性和安全性等特点，目前在大型DBMS的权限管理中得到普遍应用。

4．基于任务的访问控制

基于任务的访问控制（Task-Based Access Control, TBAC）通过授权步的动态权限管理，TBAC支持最小特权原则和最小泄露原则，在执行任务时只给用户分配所需的权限，未执行任务或任务终止后用户不再拥有所分配的权限；在执行任务过程中，当某一权限不再使用时，授权步自动将该权限回收。TBAC适用于工作流、分布式处理、多点访问控制的信息处理和事务管理系统，最显著的应用是在安全工作流管理系统中。

5．基于对象的访问控制

控制策略和控制规则是基于对象的访问控制（Object-based Access Control, OBAC）的核心，在OBAC模型中，将ACL与受控对象及其属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合。同时，允许对策略和规则进行复用、继承和派生操作。这样，不仅可以对受控对象本身进行访问控制，受控对象的属性也可以进行访问控制，而且派生对象可以继承父对象的访问控制设置，这对于信息量巨大、信息内容更新变化频繁的管理信息系统非常有益，可以减轻由于信息资源的派生、演化和重组等带来的分配和设定角色权限等的工作量。

技术成就梦想