***第一章:绪论***

习近平指出：没有网络安全就没有国家安全。人类已经进入信息的时代，信息已成为一种重要的战略资源，信息技术也成为了衡量国家竞争力的重要标志。

* 1. **信息安全的概念**：信息：事物运动的状态和状态变化的方式。信息安全：指信息系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，信息系统连续、可靠、正常地运行，信息服务不中断。信息安全的目标是保护网络与信息系统中信息的机密性、完整性、不可抵赖性、可用性和可控性等信息安全属性。机密性、完整性、可用性也称为信息安全的三要素。其他的信息安全属性与这3个要素密切相关、或可以从这3个要素导出。信息安全属性：（1）机密性能够确保敏感数据或机密数据在存储和传输过程中不被非授权的实体浏览，甚至可以保证不暴露保密通信的事实。•通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。(2)完整性能够保障被传输、接收、存储的数据是完整和未被非法修改的，在被非法修改的情况下能够发现被非法修改的事实和位置。•一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。信息的完整性包括数据和系统的完整性。(3)真实性•参与通信或操作的实体（用户、进程、系统等）身份的真实以及信息来源的是否真实。确保实体就是所声称的实体。技术：标识和认证(4)不可否认性•实体的行为或事件的结果是不能被否认的。能够保证信息系统的操作者和信息的处理者不能够否认其操作行为和处理结果，防止参与操作或通信的某一方事后否认该操作和通信行为的发生。•技术：审计和日志，数字签名和安全协议(5)可靠性•信息系统运行的过程和结果是可以被信赖的。通常用平均无故障时间来描述；如果系统被黑客控制，则不可靠。(6)可用性•当突发事件（故障、攻击等）发生时，用户依然能够得到或使用信息系统的数据，信息系统的服务亦能维持运行。•可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息。•可用性是信息资源服务功能和性能可靠性的度量，涉及到物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。(7)可控性•能够掌握和控制信息及信息系统的情况，对信息和信息系统的使用进行可靠的授权、审计、责任认定、传播源与传播路径的跟踪和监管等。技术：访问控制(8)保鲜性(新鲜性)•也就是说信息必须是在其时效之内的，不能是过时的。新鲜性对保证物联网的安全尤其重要。信息安全威胁：信息安全可被理解为信息系统抵御信息安全威胁，保证信息系统处理维护的数据以及提供的服务的机密性、完整性、真实性、不可否认性、可靠性、可用性、可控性等安全属性的能力。•所谓信息安全威胁，就是对信息资源或信息系统的安全使用可能造成的危害，主要包括意外事件和人为恶意攻击两大类。精心设计的人为恶意攻击的威胁最大。•信息安全威胁也可以理解为某个人、物、事件或概念对信息资源的保密性、完整性、可用性或合法使用所造成的危险。包括：(1)信息泄露•保护的信息被泄露或透露给某个非授权的实体。•典型攻击手段是窃听和通信业务流分析。窃听是指用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息，例如对通信线路中传输的信号搭线监听；通信业务流分析则通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。(2)非授权的篡改•信息的内容被非授权地进行增删、修改或破坏而受到损失。(3)拒绝服务•信息使用者对信息或其他资源的合法访问被无条件地阻止。如：分布式拒绝服务攻击。(4)非法使用（非授权访问）•某一资源被某个非授权的人或系统使用，或以非授权的方式使用（越权使用）。(5)假冒•一个非法用户或信息系统通过冒充成为另一个合法用户或合法系统，或者特权小的用户／系统冒充成为特权大的用户／系统。(6)抵赖•一种来自用户的攻击，涵盖范围比较广泛。比如，否认自己曾经发布过的某条消息，否认曾经处理过某些信息等。(7)网络与系统攻击•利用网络系统和协议的缺陷和漏洞，进行恶意的侵入和破坏。比如，缓冲区溢出攻击。(8)恶意代码•开发、传播意在破坏计算机系统、窃取机密或远程控制的程序，主要包括计算机病毒、蠕虫、木马、僵尸网络等。比如，恶意网站的恶意网页。(9)自然灾害•如火灾、水灾等意外事件，损毁、破坏信息系统的硬件设备，从而使得信息和信息系统不可用。(10)人为失误和故意破坏•恶意的人故意破坏，或者授权用户的操作失误，使得信息或信息系统遭到损坏。•安全威胁分别破坏不同的信息安全属性。**1.2信息安全发展历程:**信息安全发展经历了4个时期：通信安全时期,计算机安全时期,网络安全时代,信息安全保障时代.。**1.3信息安全技术体系：**1)信息安全保障技术框架其基本内容是深度防御策略、信息保障框架域和信息系统安全。必须全面考虑人、技术和操作（与管理）这三个要素。2)密码技术密码技术主要包括密码算法和密码协议的设计与分析技术。•密码算法包括分组密码、序列密码、公钥密码、杂凑(哈希)函数、数字签名等，它们在不同的场合分别用于提供机密性、完整性、真实性、可控性和不可否认性，是构建安全信息系统的基本要素。•密码协议是在消息处理环节采用了密码算法的协议，它们运行在计算机系统、网络或分布式系统中，为安全需求方提供安全的交互操作。•密码分析技术指在获得一些技术或资源的条件下破解密码算法或密码协议的技术。其中资源条件主要指分析者可能截获了密文、掌握了明文或能够控制和欺骗合法的用户等。。3)标识与认证技术标识是指实体的表示，信息系统通过标识可以对应到一个实体。•认证技术就是鉴别实体身份的技术，主要包括口令技术、公钥认证技术、在线认证服务技术、生物认证技术与公钥基础设施技术等，还包括对数据起源的验证。4)授权与访问控制技术为了使得合法用户正常使用信息系统，需要给已通过认证的用户授予相应的操作权限，这个过程被称为授权。•在信息系统中，可授予的权限包括读／写文件、运行程序和网络访问等，实施和管理这些权限的技术称为授权技术。访问控制技术和授权管理基础设施技术是两种常用的技术。5)信息隐藏技术信息隐藏是指将特定用途的信息隐藏在其他可公开的数据或载体中，使得它难以被消除或发现。•信息隐藏主要包括隐写、数字水印与软硬件中的数据隐藏等，其中水印又分为鲁棒性水印和脆弱性水印。6)网络与系统攻击技术网络与系统攻击技术是指攻击者利用信息系统弱点(vulnerability，漏洞)破坏或非授权地侵入网络和系统的技术。•主要的网络与系统攻击技术包括网络与系统调查、口令攻击、拒绝服务攻击、缓冲区溢出攻击等。拒绝服务攻击是指攻击者通过发送大量的服务或操作请求使服务程序 出现难以正常运行的情况；缓冲区溢出攻击属于针对主机的攻击，它利用了系统堆栈结构，通过在缓冲区写入超过预定长度的数据造成所谓的溢出，破坏了堆栈的缓存数据，使程序的返回地址发生变化。7)网络与系统安全防护及应急响应技术网络与系统安全防护技术就是抵御网络与系统遭受攻击的技术，它主要包括防火墙和入侵检测技术。8)安全审计与责任认定技术为抵制网络攻击、电子犯罪和数字版权侵权，安全管理部门或执法部门需要相应事件的调查方法与取证手段，这种技术被统称为安全审计与责任认定技术。9)主机系统安全技术10)网络系统安全技术主要包括提供传输层安全的系统、提供网络层安全的IPSec系统及提供应用层安全的安全电子交易SET系统。11)恶意代码检测与防范技术12)内容安全技术13)信息安全测评技术14)信息安全管理技术**1.4 信息安全模型：**信息安全模型也被称为威胁模型或敌手模型。包括：Shannon提出的保密通信系统的模型，Simmons面向认证系统提出了无仲裁认证模型，Dolev-Yao威胁模型。**1.5信息安全保障技术框架：**IATF的核心思想IATF提出的信息保障的核心思想是纵深防御战略。所谓纵深层防御战略就是采用一个多层次、纵深的安全措施来保障用户信息及信息系统的安全。在纵深防御战略中，人、技术和操作是三个主要核心要素，要保障信息及信息系统的安全，三者缺一不可。IATF的其他信息安全(IA)原则：(1)保护多个位置(2)分层防御(3)安全强健性。

***第二章:密码技术***

**2.1 基本概念**密码学=密码编码学+密码分析学•密码编码学：研究密码变化的客观规律，设计各种加密方案，编制密码以保护信息安全的技术。•密码分析学（或密码破译学）：在不知道任何加密细节的条件下，分析、破译经过加密的消息以获取信息的技术。•明文：原始的消息•密文：加密后的消息明文到密文的变换法则，即加密方案，称为加密算法；而密文到明文的变换法则称为解密算法。加／解密过程中使用的明文、密文以外的其他参数，称为密钥。密码体制：一个用于加解密并能够解决网络安全中的机密性、完整性、可用性、可控性和真实性等问题中的一个或几个的系统。•密码体制可以定义为一个五元组(P,C,K,E,D)P称为明文空间，是所有可能的明文构成的集合；C称为密文空间，是所有可能的密文构成的集合；K称为密钥空间，是所有可能的密钥构成的集合；E和D分别表示加密算法和解密算法的集合，它们满足：•对每一个k∈K，必然存在一个加密算法ek∈E和一个解密算法dk∈D，使得对任意m∈P，恒有dk(ek(m))=m。对称密码体制也叫单钥密码体制或秘密密钥密码体制：在对称密码体制中，加密和解密使用完全相同的密钥，或者加密密钥和解密密钥彼此之间非常容易推导。•非对称密码体制也称为公钥（公开密钥）密码体制：在公钥密码体制中，加密和解密使用不同的密钥，而且由其中一个推导另外一个是非常困难的。这两个不同的密钥，往往其中一个是公开的（公钥，通常用于加密），而另外一个保持秘密性（私钥，通常用于解密）。密码体制的安全性尽量满足：(1)破译密码的代价超出密文信息的价值。(2)破译密码的时间超出密文信息的有效生命期。攻击密码体制的两种方法：（1）密码分析攻击：①唯密文攻击②已知明文攻击③选择明文攻击④选择密文攻击（强度依次增强）（2）穷举攻击**2.2 对称密码**在对称密码体制中，加密和解密使用完全相同的密钥，或者加密密钥和解密密钥彼此之间非常容易推导。对称密码包括：古典密码与分组密码和序列密码。古典密码技术以字符为基本加密单元，现代密码学的两大基本思想：置换和代换。置换技术：保持明文中的字母本身不变，但将所有字母重新排列，即仅仅改变明文字母的位置，这样的密码技术称为置换。代换技术：所谓代换，是将明文字母用其他字母、数字或符号替换的一种方法。为此，要建立一个或多个替换表，这些替换表就是密钥。**2.2.2 分组密码**对称密码分为两大类：流密码和分组密码①流密码又称作序列密码，加密和解密每次只处理数据流的一个符号（如一个字符或一个比特）。古典密码都属于流密码。②分组密码又称块密码，它将明文消息划分成若干长度为m(m>1)的分组（或块），各组分别在长度为r的密钥K的控制下转换成长度为n的密文分组。如果m>n，则称为带数据压缩的分组密码，可以增加密文解密的难度；如果m<n，则称为带数据扩展的分组密码，其密文存储和传输的代价较大。绝大部分基于网络的对称密码应用使用的是分组密码。DES分组长度为64位，密钥长度为56位。步骤：①变换明文②按照规则迭代③逆置换。DES的安全性：DES收到的最大攻击是它的密钥长度仅有56比特（密钥的长度和算法本身的安全性）。**2.2.3 序列密码：**序列密码的加密和解密每次只处理数据流的一个符号。**2.3 公钥密码**在传统的对称密码体制中，当通信的用户数目比较多的时候，密钥的产生、存储和分发是一个很大的问题。公钥密码体制将加密密钥和加密函数公开。任何人都可以加密，但只有掌握解密密钥的用户才能解密。•公钥密码体制不仅用于加解密，而且可以广泛用于消息鉴别、数字签名和身份认证等服务对数据的加解密使用对称密码技术，而密钥管理使用公钥密码技术。**2.3.1 公钥密码体制原理**①公钥算法建立在数学函数基础上，安全性为数学上难解的问题。②由一个密钥推至另一个密钥，理论上是不可能的。③通信双方无需预先商定密钥就可以进行秘密通信。公钥密码算法的重要特点1.加密／解密使用不同的密钥；2.发送方拥有加密密钥或解密密钥，而接收方拥有另一个密钥；3.根据密码算法和加密密钥以及若干密文，要恢复明文在计算上是不可行的；4.根据密码算法和加密密钥，确定对应的解密密钥在计算上是不可行的。公钥密码体制是建立在单向陷门函数的基础上。**2.3.2RSA算法**是一种分组密码体制，理论基础为大整数的素因子分解是困难问题。密钥计算方法：①选择两个大素数p和q②计算n=p\*q和z=(p-1)\*(q-1)③选择一个与z互质的数，令其为d④找到一个e使满足e\*d=1(modz)⑤公开密钥为(e,n)，私有密钥为(d,n)。加密方法： ① 将明文看成比特串，将明文划分成k位的块P即可， 这里k是满足2 k<n的最大整数。 ② 对每个数据块P，计算C＝P^ e (mod n)，C即为P的密文。 • 解密方法： ➢对每个密文块C，计算P＝C ^d (mod n)，P即为明文。**2.4 散列函数和消息认证码**散列函数又叫做散列算法，是一种将任意长度的消息映射到某一固定长度消息摘要（散列值或哈希值）的函数。可以验证该消息的完整性。散列函数的安全性：单向性，强抗碰撞性和弱抗碰撞性。**消息鉴别码**：保障消息完整性和真实性的重要手段是消息鉴别技术。过程：用鉴别函数产生一个鉴别符，根据收发端的鉴别符是否一致，对消息进行鉴别。鉴别函数分为三类：基于消息加密、基于消息鉴别码、基于散列函数。基于Hash函数导出MAC的方法成为了主流。1）基于MAC的鉴别：消息鉴别码又称密码校验和原理是：利用公开函数和密钥生成一个固定大小的小数据块，即MAC，并将其附加在消息之后传输。接收方利用与发送方共享的密钥进行鉴别。数据鉴别算法，也称为CBC-MAC(密文分组链接消息鉴别码) **2.5 数字签名** 签名起到了鉴别、核准、负责等作用，表明签名者对文档内容的认可，并产生某种承诺或法律上的效力。数字签名是手写签名的数字化形式。数字签名的基本目的是认证、核准和负责，防止相互欺骗和抵赖。形式化定义：一个数字签名体制是一个五元组(M，A，K，S，V)，其中：※M是所有可能的消息的集合，即消息空间。※A是所有可能的签名组成的一个有限集，称为签名空间。※K是所有密钥组成的集合，称为密钥空间。※S是签名算法的集合。※V是验证算法的集合。数字签名必含的4个特征：①可验证性②不可伪造性③不可否认性④数据完整性。基于公钥密码算法和对称密码算法都可以获得数字签名，目前主要是基于公钥密码算法的数字签名。**2.6 密钥管理** 密码系统的安全性就完全取决于密钥的保密程度。密钥管理的核心问题是：确保密钥从产生到使用全过程的安全可靠。密钥的类型(1)工作密钥(2)会话密钥(3)密钥加密密钥(4)主机主密钥。

**Hw数字签名和消息鉴别的主要区别**：数字签名的基本目的是认证、核准和负责，防止相互欺骗和抵赖。可处理双方内部的攻击；消息鉴别为了保证消息的完整性和真实性，但不能处理双方内部的攻击。

***第三章 身份认证***

**身份认证**：确认某个实体是所声称的实体的行为。包括两种情况：①计算机认证人的身份，称之为用户认证②计算机认证计算机，称之为认证协议。**3.1 用户认证** 用户向计算机系统出示自己的身份证明，以便计算机系统验证确实是所声称的用户。用户认证是对访问者授权的前提。**3.1.1 基于口令的认证** ①静态口令：需解决的两个问题：1）口令存储：如果口令以明文方式存储，则易受字典攻击，一般系统的口令文件存储的是口令的散列值，攻击者难于得到口令明文2）口令传输：一般采用双方协商好的加密算法或单向散列函数对口令进行处理后传输。静态口令的认证方式存在的安全问题：①它是一种单因素的认证方式，安全性全部依赖于口令，口令一旦被泄露，用户即可被冒充。②为了便于记忆，用户往往选择简单、容易被猜测的口令。这使得口令被攻击的难度大大降低。③口令在网络上传输的过程中可能被截获。④系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件。⑤用户在访问多个不同安全级别的系统时，都要求用户提供口令，用户为了记忆的方便，往往采用相同的口令。⑥口令方案无法抵抗重放攻击。⑦只能进行单向认证，即系统可认证用户，而用户无法对系统进行认证，攻击者可能伪装成系统骗取口令。②动态口令：动态口令又叫做一次性口令，是指在用户登录系统进行身份认证的过程中，送入计算机系统的验证数据是动态变化的。•动态口令的主要思路是在登录过程中加入不确定因素，如时间。系统执行某种加密算法E(用户名+密码+不确定因素(时间))，产生一个无法预测的动态口令，以提高登录过程的安全性。动态口令的产生：1)共享一次性口令表2)口令序列3)挑战—响应方式4)时间—事件同步机制。基于电子令牌卡生成口令的工作原理：A.用户和计算机系统之间共享同一个用户口令。用户还拥有一种叫做动态令牌的专用硬件B.当用户向认证系统发出登录请求时，认证系统向用户发送挑战数据。C。用户接收到挑战后，将种子值、随机数值和用户口令输入到动态令牌中进行计算，并把结果作为应答发送给远程认证系统。动态口令的技术特点：动态性、随机性、一次性、方便性。**3.1.2 基于智能卡的认证** 智能卡是一种集成的带有智能的电路卡，内置可编程的微处理器，可存储数据，并提供硬件保护措施和加密算法。 USB KEY是一种USB接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书。USB Key主要特点：（1）双因子认证。每个USB Key都具有硬件和PIN码保护。（2）带有安全的存储空间（3）硬件实现加密算法（4）便于携带、安全可靠。基于USB Key的身份认证主要方式：（1）基于挑战/应答的双因子认证方式（2）基于数字证书的认证方式，数字证书是由权威公正的第三方机构（即CA中心）签发的，由用户的身份与其所持有的公钥相结合的计算机文件。**数字证书的基本功能：**以数字证书为核心的加密技术，可以对网络上传输的信 息进行加密、解密、数字签名和签名验证，确保网上传 递信息的机密性、完整性，以及交易实体身份的真实性， 签名信息的不可否认性，从而保障网络应用的安全性。 **3.1.3 基于生物特征的认证** 基于生物特征识别的认证方式以人体具有的唯一的、可靠的、终生稳定的生物特征为依据。具有以下优点：①不易遗忘或丢失。②防伪性能好，不易伪造或被盗。③“随身携带”，方便使用。**3.2 认证协议** 认证协议通过一定的过程，保证使合法的协议一方（或双方彼此）确信对方确实是其所声称的 那个实体。身份认证协议的实质是抗身份欺诈。3.2.1 单向认证 单向认证是指通信双方中，只有一方对另一方进行认证。单向认证(B认证A)协议包括三个步骤： ① 应答方B通过网络发送一个挑战； ② 发起方A回送一个对挑战的响应； ③ 应答方B检查此响应，然后再进行通信。每个用户与密钥分配中心(KDC)共享唯一的主密钥（KDC干预）。**3.2.2 双向认证** 双向认证指通信双方相互验证对方的身份。 • 双向认证协议可以使通信双方确信对方的身份 并交换会话密钥。保密性和及时性是认证的密钥交换中两个重要的问题。对付重放攻击的两种方法：时间戳、挑战\应答。应对重放攻击的2种方法的适用场合：时间戳方法不适合于面向连接的应用；另一方面，挑战／应答不适合于无连接的应用。**3.3 Kerbeross** 是MIT开发的一种基于对称密码算法的网络认证协议，允许一个非安全的网络上的两台计算机通过交换加密消 息互相证明身份。一旦身份得到验证，Kerberos协议给这两台计算机提供密钥，以进行安全的通信。Kerberos的设计目的：解决分布式网络环境下，用户访问网络资源时的安全问题。Kerberos是为TCP/IP网络设计的可信第三方认证协议，利用可信第三方KDC(密钥分配中心)进行集中的认证。 **3.3.1 Kerberos版本4** Kerberos的设计目的是使用户通过用户名和口令登录到工作站，工作站基于口令生成密钥，并使用密钥和KDC联系，以代替用户获得远程资源的使用授权。**1. 版本改进** Kerberos版本5对版本4存在的一些缺陷进行了改进，包括：1)加密系统依赖性2)Internet协议依赖性3)消息字节顺序4)门票的生命期5)向前认证6)域间认证7)冗余加密8)PCBC加密9)会话密钥 **3.4 PKI技术**PKI:公钥基础设施 • PKI是一种遵循标准的、利用公钥加密技术的一套安全基础平台的技术和规范。 **3.4.1 PKI体系结构** • 简单的说，PKI是基于公钥密码技术，支持公钥管理，提供真实性、保密性、完整性以及可追究性安全服务，具有普适性的安全基础设施。•PKI的核心技术围绕建立在公钥密码算法之上的数字证书的申请、颁发、使用与撤销等整个生命周期进行展开，主要目的就是用来安全、便捷、高效地分发公钥。IETF的PKI小组制订了一系列的协议，定义了基于X.509证书的PKI模型框架，称为PKIX。PKI应用系统的组成：认证机构(CA)：CA是PKI 的核心执行机构，是PKI 的主要组成部分，人们通 常称它为认证中心。数字证书库：证书库是 CA颁发证书和撤销证书的集中存放地，可供公众进行开放式查询。密钥备份及恢复系统：密钥备份与恢复只能针对解密密钥，签名私钥为确保其唯一性而不能够作备份。证书作废系统：作废证书一般通过将证书列入作废证书表 (CRL)来完成。应用接口(API)。**3.4.2 X.509数字证书** 包含以下信息：*(1) 版本号(2) 序列号(3) 签名算法标识(4) 签发者(5) 有效期(6) (7) 证书主体的公钥信息证书主体名(8) 签发者惟一标识(9) 证书主体惟一标识(10) 扩展(11) 签名*。**3.4.3 认证机构** CA的主要职能：*①制定并发布本地CA策略。但本地策略只是对上级CA策略的补充，而不能违背。②对下属各成员进行身份认证和鉴别。③发布本CA的证书，或者代替上级CA发布证书。④产生和管理下属成员的证书。⑤证实RA的证书申请，返回证书制作的确认信息，或返回已制作的证书。⑥接收和认证对所签发证书的撤销申请。⑦产生和发布所签发证书和CRL。⑧保存证书、CRL信息、审计信息和所制定的策略。***3.4.4 PKIX相关协议** 在PKIX中，不可抵赖性通过数字时间戳DTS和数据有效性验证服务器DVCS实现。**3.4.5 PKI信任模型** 所谓信任模型，就是提供用户双方相互信任机 制的框架，是PKI系统整个网络结构的基础。包含：①层次模型②交叉模型③混合模型④桥CA模型⑤信任链模型。*如何保证根证书可信？Ans：①购买计算机带着操作系统隐含着对操作系统的信任，操作系统提供最初的安装中能保证根证书可信②操作系统可信，通过浏览器在可信网站下载软件，自带根证书软件导入操作系统后可信③通过可信网站直接下载相关证书，且下载的证书与上一级原证书进行验证。④从发行方手中获得可信证书。*

***第四章 授权与访问控制技术***

**4.1 授权和访问控制策略的概念** 给已通过认证的用户授予相应的权限，这个过程被称为授权。目前，主要有两种授权技术，即访问控制技术和PMI技术。在信息系统中，资源主要指信息数据、计算处理能力和网络通信资源等。在访问控制中，通常将它们称为客体。**相关的概念**：访问”一词可以概括为系统或用户对这些资源的使用，如读取数据、执行程序、占用通信带宽等，这些“访问者”通常被称为主体，而有的实体既可以作为主体，也可以作为客体，如计算机程序，因此也常用实体统一指代客体和主体。• 授权是指资源的所有者或控制者准许别的主体以一定的方式访问某种资源，访问控制是实施授权的基础，它控制资源只能按照所授予的权限被访问。• 访问控制策略是在系统安全较高层次上对访问控制和相关授权的描述，它的表达模型常被称为访问控制模型，是一种访问控制方法的高层抽象和独立于软硬件实现的概念模型。1）主体属性 用户的级别或种类是主要的主体属性。 • 操作系统一般将用户分为多种普通用户和管理员用户，用户还可以分成组，因此具有组别属性。在其他系统中，用户被授予各种角色属性，如是局长或科员。 • 主体属性还可能包括相关执行程序的性质、所处的网络或物理地址等，它们也可能是授权的依据。 • 例如，很多单位规定，从家中不能访问办公室的资源。 • 在安全性要求更高的情况下，主体的属性可能还包括其安全状态。2）客体属性 客体的主要属性是所允许的操作及其信息级。别客体的属性也可能包括其安全状态。**4.2 自主访问控制** 在自主访问控制中，由客体的所有者（或控制者）对自己的客体进行管理，由所有者 决定是否将自己客体的访问权或部分访问权授予其他主体。 • 一般地，自主访问控制策略是基于主体的身份和先行规定的访问规则来对访问进行控制。 自主访问控制在(可信计算机评价标准(TCSEC)的)C2级操作系统中应用广泛，是根据自主访问控制策略建立的一种模型，允许合法用户以用户或用户组的身份访问策略规定的客体， 同时阻止非授权用户访问客体，某些用户还可以自主地把自己所拥有的客体的访问权限授予其他用户。**4.2.1 基本概念：**自主访问控制策略根据来访主体的身份，来实施访问控制。之所以被称为自主策略，是因为它基于这样的思想：客体的主人（即资源所有者） 全权管理有关该客体的访问授权，有权泄露、修改该客体的有关信息。**1.传统DAC策略** 特点：访问权限的管理依赖于所有对客体具有访问权限的主体。不足：① 资源管理比较分散。 ② 用户间的关系不能在系统中体现出来，不易管理。 ③ 不能对系统中的信息流进行保护，容易泄露，无法抵御特洛伊木马。**2.HRU、TAM、ATAM策略** HRU与传统 DAC最大的不同在于它将访问权限的授予改为半自主。访问权限的授予行为要受到一个调整访问权限分配的安全策略的限制。TAM策略对HRU模型的改进：当主体集和客体集发生改变时，需要依赖安全管理员对访问权限的扩散策略进行更新。**3．基于角色／时间特性的DAC策略** 核心思想：增加角色，实现更细粒度的访问控制。**4.2.2 授权管理** 自主访问控制的授权管理大致有以下几种：①集中式管理②分级式管理③所属权管理④协作式管理⑤分散式管理。访问控制实现技术：①保护位机制②能力表机制③访问控制表机制④授权关系表机制 **4.2.3 自主访问控制不足之处** • (1)既然用户可任意在系统中规定谁可以访问它们的资源， 那么系统管理员就难以确定哪些用户对哪些资源有访问权限，不利于实现统一的全局访问控制。 • (2)由管理部门统一实施访问控制，DAC却存在用户滥用职权的问题。 • (3)用户间的关系不能在系统中体现出来，不易管理。 • (4)信息容易泄露，不能抵御特洛伊木马的攻击。(5)自主访问控制存在安全风险，风险又分为三个类型，即自由型、等级型、宿主型。在这些系统中，位于树型结构顶端的超级用户拥有无上的权限，可以对其他用户拥有的资源 进行任意修改和访问。权限的高度集中，客观上放大了系统的安全风险。**4.2.4 完善自主访问控制机制** 要求：客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。从技术要求的细节上看，满足等级保护标准的自主访问控制机制实质上是宿主型自主访问控制。用户需要对客体设置一个拥有者，并使其成为唯一有权访问该客体访问控制表的主体。**4.3 强制访问控制** 在强制访问控制(mandatory access control，MAC) 中，用户和客体资源都被赋予一定的安全级别， 用户不能改变自身和客体的安全级别，只有管理员才能够确定用户和组的访问权限。强制访问控制策略是基于系统权威（如安全管理员）制定的访问规则来对访问进行控制，如多级安全MLS。**4.3.1 基本概念** 强制访问控制模型基于与每个数据项和每个用户关联的安全性标识。安全性标识被分为若干级别：绝密、机密、秘密、一般。数据的标识称为密级，用户的标识称为许可证级别。确定该用户能否访问系统上的数据时应遵守如下规则： (1)当且仅当用户许可证级别大于或等于数据的密级时，该用户才能对该数据进行读操作。 (2)当且仅当用户许可证级别小于或等于数据的密级时，该用户才能对该数据进行写操作。这两种规则的共同点在于它们禁止了拥有高级许可证级别的主体更新低密级的数据对象，从而防止了敏感数据的泄露。**强制访问控制的主要特征：**强制访问控制(MAC)的主要特征是权威制定访问规则，对所有主体及其所控制的客体（进程、文件、段、设备等）实施强制访问控制。访问控制是“强加”给访问主体的，即系统强制主体服从访问控制策略。用户的程序不能改变他自己及任何其他客体的敏感标记。**强制访问控制策略**：多级安全策略是最为常见的强制访问控制策略，它基于系统中主体与客体的分级来决定是否允许访问。**主体对客体的4种访问方式**：(1)向下读(2)向上读(3)向下写(4)向上写。 **4.3.2 授权管理**在强制访问控制中，访问控制完全是根据主体和客体的安全级别决定。只有安全管理员能够改变主体和客体的安全级别。**4.3.3 不足之处** 强制访问控制策略去除了自主访问控制策略中由用户来自由分配的特点，而采用集中控制的方法。MAC也存在一些不足之处，主要表现：(1)完整性方面控制不够(2)应用领域比较窄，无法适应复杂的现实环境。**4.4 基于角色的访问控制** DAC和MAC这两种访问控制模型都存在的不足是将主体和客体直接绑定在一起，授权时需要对每对（主体、客体）指定访问许可，这样存在的问题是当主体和客体达到较高的数量级之后，授权工作将非常困难。**4.4.1 基于角色的访问控制RBAC的基本概念 基本思想**：对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合，每一种角色对应一组相应的权限。**RBAC的核心思想**是将权限与角色联系起来，在系统中根据应用的需要为不同的工作岗位创建相应的角色。同时根据用户职责指派合适的角色，用户通过所指派的角色获得相应的权限，实现对文件的访问。RBAC在中间加入角色，通过角色沟通主体和客体。**RBAC的基本思想：**授权给用户的访问权限，通常由用户在一个组织中担当的角色来确定。RBAC中许可被授权给角色，角色被授权给用户，用户不直接与许可关联。RBAC对访问权限的授权由管理员统一管理，用户不能自主地将访问权限传给他人。**好处：**简化了授权管理，具有强大的可操作性和可管理性。RBAC属于策略中立型的存取控制模型，既可以实现自主存取控制策略，又可以实现强制存取控制策略。基于角色访问控制根据对合法的访问者进行角色认证来确定访问者在系统中对哪类信息有什么样的访问权限。**基于角色访问控制策略中的关键概念：**(1)主体：可以对其他实体实施操作的主动实体(2)客体：接受其他实体动作的被动实体• (3)用户：试图使用系统的人员。每个用户都有一个唯一的用户标识(UID)。RBAC用户**：**①普通的用户②特殊的用户③作废的用户④作审计的用户（4）角色**：**是系统中一组职责和权限的集合。(5)权限：在收系统保护的客体上执行某一操作许可。用户对特定的资源进行特定操作的许可称为权限。(6)用户角色分配:为用户分配一定的角色，即建立用户与角色的多对多关系。(7)角色权限分配:为角色分配一组访问权限。(8)会话:一次会话是用户的一次活跃进城，它代表用户与系统进行交互。(9)活跃角色集:一个会话构成一个用户到多个角色的映射，即会话激活了用户授权角色集的某个子集。(10)保护域:保护域是一系列权限的集合，描述一个主体在给定时间可能执行的所有操作的集合。**4.4.2 授权管理** 授权是指可以授予角色或用户的独立权限，授权在用户中的应用程序级别强制执行策略。依据角色指派关系，运行系统中的用户自身可以对角色进行管理。通常，角色指派的权力都在系统中具有管理责任的用户手中。在增强RBAC中，授权是与安全相关的功能或者命令相关联的文本字符串。授权提供了一种机制，以便为用户授予相应的权限以执行某些特权操作，并对不同类别的用户提供不同的功能级别。特权在内核中强制执行安全策略，授权与特权之间的差别与强制执行安全策略的级别有关。**2.授权策略** 授权策略规定何人在何种情况下能访问何种目标访问控制和授权策略展示了一个机构在信息安全和授权方面的顶层控制。**授权策略的基本内容:**(1)委托策略(2)SOA（信任源）策略(3)角色指派策略• (4)动作策略(5)用户策略(6)目标访问策略(7)角色继承策略 **4.4.3 RBAC的优势** (1)简化权限管理• (2)灵活表达和实现组织的安全策略• (3)安全性高。该策略可以有效实现最小权限管理。(4)实用性强 **4.5 基于属性的访问控制（ABAC）**基于属性的访问控制(ABAC)有效解决了具有大规模、强动态性和强隐私性特点的新型计算环境下的细粒度访问控制问题，为云计算、物联网等新型计算环境提供了理想的访问控制策略。•ABAC将主体和客体属性作为决策的基本依据，灵活地利用资源访问者所具有的属性决定是否授予其访问权限，能够很好地将策略管理和权限判定分离。**4.5.1 ABAC模型** 四元组(S，O，P，E)①S表示主体属性②O表示客体属性③P表示权限属性④E表示环境属性。**ABAC的不足之处**①用户的身份具有较强的匿名性，导致可能滥用其所拥有的的属性带来的权限。同时，新型计算环境中用户和设备的动态特性带来了权限的频繁变动，需要对这些变动实时响应，更改相应的权限，保证系统安全可靠的运行。**4.5.2 ABE的基本概念** 虽然传统的ABAC有效控制了用户对资源的访问操作，但其仅实现了对用户访问过程的控制。 • 随着云计算和物联网等新型计算环境产生以及存储的敏感隐私信息日益增多，由信息泄露所导致的安全威胁也不断增加。因此，为了最大限度的保护数据的隐私安全，实现更细粒度的访问控制，研究者们提出了基于属性的加密机制(ABE)。ABE实现了对数据机密性的访问控制，其采用非对称密码机制并利用属性作为加解密的关键要素，将属性同密文和用户密钥相结合。KP-ABE（基于密钥策略的ABE）方案中，用以描述访问控制策略的访问结构同用户私钥相结合，属性集合同待访问资源相关联。而CP-ABE（基于密文策略的ABE）方案则与KP-ABE相反，此时用以描述访问控制策略的访问结构同待访问资源相结合，属性集合同用户私钥相关联。**ABE机制的不足之处** ABE机制中的权限更新问题尤为突出。 • 如何平衡更新粒度及计算资源消耗的权限更新机制是ABE中的重要问题。**4.6 PMI技术 4.6.1 PMI基础**PMI(privilege management infrastructure)即权限管理基础设施或授权管理基础设施，是属性证书、属性权威、属性证书库等部件的集合体，用来实现权限和证书的产生、管理、存储、分发和撤销等。 • AA即属性权威，是用来生成并签发属性证书的机构。它负责管理属性证书的整个生命周期。 • AC即属性证书，对于一个实体的权限的表示是由一个进行了数字签名的数据结构来提供的，这种数据结构称为属性证书，由属性权威签发并管理。**PMI以资源管理为核心**：建立在PKI基础之上的PMI，以向用户和应用程序提供权限管理和授权服务为目标，PMI以资源管理为核心，对资源的访问控制权交由授权机构统一处理，即由资源的所有者来进行访问控制。PKI证明用户是谁，而PMI证明这个用户有什么权限，能干什么，而且PMI需要PKI为其提供身份认证。**4.6.2 PKI与PMI的关系**PMI主要进行授权管理，证明这个用户有什么权限，即“你能做什么”； • PKI主要进行身份鉴别，证明用户身份，即“你是谁” 。• PKI和PMI的关系类似于签证和护照的关系。PKI信任源有时被称为根CA，而PMI信任源被称为SOA。**4.6.3 PMI授权管理模式、体系及模型 1.PMI技术的授权管理模式** 授权服务体系主要是为网络空间提供用户操作授权的管理，即在虚拟网络空间中的用户角色与最终应用系统中用户的操作权限之间建立一种映射关系。 • 授权服务体系一般需要与信任服务体系协同工作，才能完成从特定用户的现实空间身份到特定应用系统中的具体操作权限之间的转换。PMI使用属性证书表示和容纳权限信息，通过管理证书的生命周期实现对权限生命周期的管理。PMI技术通过数字证书机制来管理用户的授权信息，并将授权管理功能从传统的应用系统中分离出来，以独立服务的方式面向应用系统提供授权管理服务。**3．PMI模型** 包括三个实体：对象、权限声称者和权限验证者。对象：可以是被保护的资源，例如，在一个访问控制应用中，受保护资源就是对象。 • 权限声明者：也就是访问者，是持有特定权限并声明其权限具有特定使用内容的实体。 • 权限验证者：对访问动作进行验证和决策，是制定决策的实体，决定被声明的权限对于使用内容来说是否充分。**4.6.4 PMI基础设施的结构和应用模型 ①**策略实施点②策略决策点③属性权威AA,属性库,策略库：属性证书AC是PMI的基本概念，属性证书的签发者被称为属性权威AA，属性权威AA的根称为SOA，属性证书被存放在属性库中。策略库主要用来存储安全授权策略数据、用户资源信息和PMI所需的相关数据。**4.6.5 属性权威与属性证书** 属性权威 • 属性权威即AA，用来生成并签发属性证书的机构，它负责管理属性证书的整个生命周期。属性证书：对于一个实体的权限的绑定是由一个进行了数字签名的数据结构来提供的，这种数据结构称为属性证书，由属性权威签发并管理。 **属性证书的特点：**公钥证书将一个身份标识和公钥绑定，属性证书将一个标识和一个角色、权限或者属性绑定（通过数字签名）。和公钥证书一样，属性证书能被分发和存储或缓存在非安全的分布式环境中，不可伪造，防篡改。属性证书具有以下特点。 (1)分立的发行机构。 (2)存储介质。属性证书可以发放给用户，由用户存储在磁盘上或者USBkey上，或者委托给系统进行统一存储和管理，而不必分发给用户。 (3)本地发放。 (4)基于其拥有属性来决定其对某一资源或服务是否拥有访 问权。 (5)属性证书可以设置成短时效的 (6)属性证书与身份证书的相互关联。4)**属性证书的分发**：推模式、拉模式。

***第五章 信息隐藏技术***

**5.1 信息隐藏的概念** 信息隐藏是把一个待保护的秘密信息隐藏在另一个称为载体的信息中，非授权者不知道这个普通的载体信息中是否隐藏了其他的信息，而且即使知道也难以提取或去除隐藏的信息。• 信息隐藏技术起源于古代的隐写术。现代信息隐藏是一种解决媒体信息安全的新方法，为数字信息的安全问题提供一种新的解决方法。这里的安全有两方面的含义：一是可公开的媒体信息在版权和使用权上的安全，二是秘密信息在传输和存储中的安全。**信息加密和信息隐藏的区别：**信息加密： • 利用密钥把信息变换成密文，通过公开信道传输。 • 如果要使用这些受保护的信息，必须有正确的解密密钥，没有密钥的非法用户无法从密文中恢复原始信息，从而无法正确使用信息。换言之，信息加密通过密钥控制信息的使用权，从而隐藏秘密信息的内容，没有密钥就无法恢复明文，但没有隐藏秘密信息存在的事实。信息隐藏： • 把秘密信息隐藏于可以公开的信息中，使攻击者难以知道秘密信息的存在，从而掩盖通信过程中存在秘密信息C事实。•其主要目的并不是限制对信息的访问，而是确保宿主信息中隐藏的秘密信息不被改变或消除，从而在必要时提供有效的证明信息。**信息隐藏技术的分类** 1. 按载体类型分类，有文本、图像、音频和视频的信息隐藏技术。 2. 按密钥分类，若嵌入和提取采用相同的密钥，则称为私钥信息隐藏技术，否则称为公钥信息隐藏技术。 3.按嵌入域分类，可分为空(间)域(或时域)和变换域方法。 4. 按检测是否需要原始载体信息参与分类，可分为非盲检测算法和盲检测算法。非盲检测算法中隐秘信息的检测需要原始载体的参与，而盲检测算法中隐秘信息的检测不需要原始载体的参与。5. 按照保护对象分类 • (1)隐写术：目的是在不引起任何怀疑的情况下秘密传送消息，因此它的主要需求包括难以检测和大容量。(2)数字水印：它是指嵌在数字产品中的数字信号，可以是图像、文字、符号、数字等一切可以作为标识和标记的信息，其目的是进行版权保护、所有权证明、指纹（追踪发布多份拷贝）和完整性保护等，因此，它的性能要求是鲁棒性和不可感知性等。• (3)数据隐藏和数据嵌入：数据隐藏和数据嵌入通常用在不同的上下文环境中，它们一般指隐写术，或者指介于隐写术和水印之间的应用。• (4)指纹和标签：这里指水印的特定用途。当前，比较活跃的信息隐藏技术主要有两个：隐写术和数字水印。**信息隐藏需满足的技术要求** (1)透明性或不可感知性：指载体在隐藏信息前后没有明显的差别，除非使用特殊手段，否则无法感知机密信息的存在。(2)鲁棒性：指隐藏对象抗拒常用的信号处理操作而带来的信息破坏能力，即常用的信号处理操作不应该引起隐藏对象的信息丢失。•(3)安全性：指隐藏算法具有较强的抗恶意攻击能力，即它必须能够承受一定程度的人为攻击而使嵌入对象不被破坏。此外，与信息加密一样，信息隐藏技术最终也需要把对信息的保护转化为对密钥的保护。•(4)不可检测性：指隐藏对象与载体对象需要有一致的特性，(5)自恢复性：经过某些操作或变换后，可能会使隐藏对象产生较大的破坏。•(6)嵌入强度(信息量)：载体中应能隐藏尽可能多的信息。 **5.2 隐藏信息的基本方法** 这些算法大多是在数字图像上发展起来的，大多数算法也适用于数字音频和视频。**典型算法如下：5.2.1 空域或像素域算法** 该类算法中最典型的是将隐秘信息嵌入到随机选择的取样点的值的最低几位上的最低有效位LSB算法。另一个常用方法是利用像素的统计特征将信息嵌入像素的亮度值中。**5.2.2 变换域算法** 此类信息隐藏算法中的大部分都基于离散余弦变换和离散小波变换。DCT变换域的基本思想是：先计算原始图像的离散余弦变换(DCT)，然后将隐秘信息叠加到变换域的系数上（不包括直流分量），这些系数通常为图像的低频分量。**DCT变换域算法的改进** ①常出现的改进是按照应用条件选择变换域②根据待隐藏的隐秘信息的类型,预编码或变形③根据隐藏信息量的大小和其相应的安全目标,选择某种变换的频域系数序列•总的来说,隐藏信息量不能很大,但抗攻击能力强,应用在数字水印技术中。**5.2.3 压缩域算法** 隐秘信息的检测与提取也可直接在数据的压缩域中进行。也就是在压缩编码算法上加入隐秘信息，而不是在DCT的系数上叠加隐秘信息。**5.2.4 NEC算法** 该算法具有较强的鲁棒性、安全性、透明性等该算法还提出了增强隐秘信息鲁棒性和抗攻击算法的重要原则，即隐秘信息应该嵌入原数据中对人感觉最重要的部分。**5.2.5 生理模型算法 5.3 数字水印 5.3.1 数字水印的技术模型** 将特定的标记嵌入到某一媒体信息中,以此实现对该媒体信息进行的某种程度的保护或监控。•水印技术主要包括水印嵌入与水印提取两个环节,信息隐藏中的密钥指的是与嵌入和提取有关的参数,如嵌入位置之类的信息,与密码技术中的密钥类似。在水印嵌入模块中,系统通过密钥的控制将水印信息嵌入原始载体数据中,形成含水印载体信息,水印的嵌入不应影响载体信息的使用价值;载体信息在公用信道中进行传输,这一过程中含水印的载体信息可能受到某种形式的信号处理或恶意攻击,形成处理或攻击后的载体信息;水印提取模块要能够从处理或攻击后的载体中正确地提取水印信息,并作为版权保护或认证的依据。 **5.3.2 数字水印的分类与应用** 1．鲁棒性水印和脆弱性水印：鲁棒性水印是指恶意攻击下仍然不能被修改、去除的水印，主要用于版权标识。脆弱性水印则是能够察觉载体信息的细微变化，并可根据被破坏的情况记录产品受到的攻击。结合鲁棒性水印、脆弱性水印和数字指纹技术所形成的综合版权管理系统可以对数字化产品同时实现版权认证、完整性认证和非法复制跟踪的保护功能。2．可见水印和不可见水印：所谓可见水印就是嵌入的保护标识是可见的，最常见的可见 水印的例子是有线电视频道或图像上的半透明标识，其主要目的在于明确标识版权，防止非法使用。不可见水印则把水印信息完全隐藏起来，目的是为了获得惩罚盗版者的证据。3．私有水印和公有水印：检测水印时必须采用原始数据作为参照的水印系统称为私有水印，而不需要采用原始数据进行检测的称为公有水印。4．对称水印和非对称水印：对称水印的嵌入与水印的提取互逆。非对称水印要求在公开水印检测算法和密钥的时候，任何人都可以方便地检测水印，但却无法根据检测算法和密钥去除已嵌入的水印信息。5.多比特水印和1比特水印。**5.3.3 空域水印** 量化水印算法也称这种算法为量化索引调制。**5.3.4 DCT域水印** 与空域图像水印相比,DCT域图像水印鲁棒性更强且与常用的图像压缩标准JPEG兼容,不是把水印加载到整幅图像上,而是随机地选取图像的一些区域加以改动以嵌入水印,一种自适应DCT域水印算法,它是基于给定灵敏度下的区域敏感性分类的,水印信号不是随机产生的。噪声敏感度的确定有许多方法,都是利用人类视觉系统的掩蔽特性**5.4 数字隐写 5.4.1 隐写的技术模型 现代隐写技术的模型** 由于对数字媒体的修改非常方便，可以根据给定的算法和密钥将秘密信息嵌入到图像、音频或视频等数字多媒体信号中，使得秘密信息在传输过程中不引起第三方或信道监控者的怀疑。接收方在得到载有秘密信息的数字载体后，可以根据提取算法和同样的密钥恢复秘密信息。秘密信息的提取一般不需要原始载体，这和一些需要载体信息作为参照的数字水印提取方法有所不同。**5.4.2 典型数字图像隐写算法** LSB算法直接用秘密信息来取代图像像素值的最低位来实现秘密信息的传递，是一种最基本的隐写方法,其他很多种流行的隐写算法大都是由其派生出来LSB隐写算法的改进:比如信息嵌入不再是简单替代,而是通过像素值规律性调整来携带信息;有的还采用了一些补偿修改来保证信息嵌入不留下明显的痕迹2自适应嵌入的隐写算法隐藏容量是隐写技术一个非常重要的指标,它要求在满足视觉不可感知的前提下,尽可能多地隐藏信息。基于位平面复杂度分割的隐写算法BPCS•PVD算法根据相邻像素的差异情况来确定图像的复杂程度。PVD,BPCS的机理均是建立在人的视觉对复杂变化的图像信号不敏感的基础之上3流行的JPEG图像隐写算法,一种较新的JPEG图像隐密算法是首先修改DCT量化步长来调整载体图像的DCT系数,在调整后的DCT系数上进行秘密信息的嵌入,此方法确实增加了隐藏容量,但量化表的调整却容易被检出异常,使其系统安全性降低4．调色板图像的隐密算法分为两大类:基于调色板的方法和基于像素索引值的方法(1)基于调色板的方法通过改变调色板中颜色的排列顺序来嵌入秘密信息。如果调色板颜色种类为N,那么排列顺序共有N!种,可以携带log2(N!)比特信息。优点是信息隐藏不会改变图像的视觉效果,其嵌入量不会随载体图像尺寸的增大而增大,同时调色板的杂乱无章也会引起监控者的怀疑,而且许多图像处理软件可以根据亮度,出现频率对调色板进行重排,这样就会删除已嵌入的秘密信息(2)利用索引色图像的像素值来携带秘密信息5．二值图像的信息隐密二值图像是一种只有黑白两种像素的特殊图像格式,对这两个反差极大的色调做直接修改很容易引起视觉异常,典型的LSB算法并不适用,针对该类载体信息,必须在信息嵌入时重点考虑视觉上的不可感知性的实现 **5.5 数字指纹** 数字指纹技术是和数字水印技术一同发展起来的新型数字版权保护技术。比较而言，数字水印是向数字产品中嵌入版权拥有者的一些信息，当发生争议时能够有效确认出版权归属，对相同的作品嵌入的水印信息是相同的。 • 而数字指纹是在原产品中嵌入与用户有关的信息，产品提供者（也称发行商）能够根据该信息对非法用户进行跟踪，嵌入的内容对不同购买者是不同的。 •通常来讲，数字指纹是指与用户和某次购买过程有关的信息。当发行商发现被非法分发的授权信息时，可以根据该信息对进行非法分发的用户实现跟踪。**数字指纹体制：**数字指纹体制主要由两部分构成：一是用于向拷贝中嵌入指纹并对带指纹拷贝进行分发的拷贝分发体制；二是实现对非法分发者进行跟踪并审判的跟踪体制。因此数字指纹体制也可以分为算法和协议两部分。**数字指纹方案应满足的基本需求:**(1)保真性(2)鲁棒性(3)嵌入量(4)合谋容忍性(5)效率。**5.5.2数字指纹编码**由于数字指纹方案要对抗用户的合谋攻击，通常发行商会对用户的指纹进行编码，以增加该指纹方案的合谋容忍能力，这种编码称为合谋容忍编码。若一个数字指纹体制能够抵抗合谋攻击，则称该指纹编码方案是合谋安全的。•指纹的合谋容忍编码通常包括两个部分：指纹的编码算法（生成带有用户指纹的拷贝）和跟踪算法(如何对非法用户进行跟踪）。•指纹编码方案：在一定假设下，将获得的与用户有关的信息按照一定的规则进行编码，生成具有一定抗攻击能力的码字的过程。•指纹跟踪方案：当发行商获得盗版拷贝时，运用一定的解码规则判断出非法分发者的过程。**指纹编码方案的分类：**①从跟踪成功的概率来讲，指纹编码方案可以分为确定性跟踪方案和概率性跟踪方案。②从码字的分布而言，可以分为连续指纹方案和离散指纹方案。③从码字是否随机来讲，还可以分为随机指纹方案和利用某些特殊的组合结构构造的指纹编码方案。**5.5.3 数字指纹协议** 类似于非对称的加密体制能够实现不可否认性， 非对称指纹体制最主要的特点是实现非法用户 的不可否认性。 非对称指纹体制一般由4个基本协议组成：①初始化协议②指纹添加协议③跟踪协议④审判协议。**匿名数字指纹：**采用这种指纹机制，用户在购买拷贝的过程中 不会泄露自己的身份信息。

***第六章 主机系统安全技术***

主机系统安全，即保证主机数据存储和处理的保密性、完整性、可用性，其核心内容包括安 全应用交付系统、应用监管系统、操作系统安全 增强系统和运维安全管控系统等。主机系统安全包括：硬件、固件、系统软件的自身安全，以及一系列附加的安全技术和安全管理措施。**6.1 操作系统安全技术 6.1.1 基本概念** 操作系统安全是主机系统安全的核心。操作系统安全是所有计算机系统安全的基石和关键。所谓安全操作系统，是在传统操作系统的基础上实现了一定安全技术的操作系统。**TCSEC6个规范性的安全要求**

1. 计算机系统必须实施一种定义清晰明确的安全策略。(2)客体必须与其访问标签相关联，以标明其安全级别。(3)主体在访问客体前必须通过严格的鉴别和认证。(4)审计信息必须单独保存，并由专门人员负责。(5)计算机系统必须能够独立评估用以实现上述(1)～(4)的软硬件机制本身的安全性。 (6)实现安全需求的可信机制自身必须受到保护，以避免被篡改或削弱。 **TCSEC的4个等级、7个级别** 1）D类安全等级 2）C类安全等级 C1（自主安全保护） C2（受控存取保护）3）B类安全等级 B1（标签安全保护） B2（结构化保护） B3（安全区域保护）4）A类安全等级（验证保护） A1（验证设计）**ITSEC和ISO15408** 欧洲四国（英、法、德、荷）提出了评价满足保密性、完整性、可用性要求的信息技术安全评价准则 (ITSEC, Information Technology Security Evaluation Criteria)后，美国又联合以上诸国和加拿大，并会同国际标准化组织（ISO）共同提出信息技术安全评价的通用准则(CC for ITSEC)，CC (Common Criteria) 已经被技术发达的国家承认为代替TCSEC的评价安全信息系统的标准。**C2安全级的关键要求：**① 安全登录机制 ② 自主访问控制机制 ③ 安全审计机制 ④ 对象重用保护机制 **Windows系统的安全机制** 实现了两项B安全技术的要求：①信任路径功能②信任机制管理。 **Windows 10 安全性概述：**(1)身份标识和访问控制 (2)信息保护 (3)防恶意软件。**6.1.3 操作系统安全的基本原理** 要 验证整个操作系统的安全性是十分困难的。所以应该使 用操作系统中尽量小的部分来提供整个操作系统的安全性，这就提出了安全核的概念。**安全核** 基于安全核构建安全操作系统具有两个方面的优势： ① 一方面能够减轻应用系统的负担，避免出现安全隐患； ② 另一方面，由于对系统的安全进行评估的内容集中在安全内核，它有利于评估的进行，使之可以进行严格的形式化验证。引用验证机制需要同时满足以下3个原则：(1)必须具有自我保护能力(2)必须总是处于活跃状态(3)必须设计得足够小，以便分析和测试。安全核是系统中与安全性的实现有关的部分， 包括引用验证机制、访问控制机制、授权机制 和授权的管理机制等。 **安全核与TCB** TCB在TCSEC中的定义是：一个计算机系统中 的保护机制的全体，它们共同负责实施一个安全策略，包括硬件、固件和软件；一个TCB由在一个产品或系统上共同实施一个统一的安全策略的一个或多个组件构成。 **可信计算基(TCB)构成** (1)固件和硬件(2)与安全策略相关的文件(3)负责安全管理的人员(4)安全核(5)具有特权的进程或命令 **TCB的基本功能** TCB的基本功能是提供敏感性数据的保密性和完整性，它必须监控操作系统内部的关于进程的活动、执行域交换以及I/O操作这三种基本行为。安全核是TCB的一个子集。**安全核在TCSEC中的定义**：一个TCB中实现引用监视器思想的硬件、固件和软件，它必须仲裁所有访问、必须保护自身免受修改、必须能被验证是正确的。 **安全操作系统的设计方法：**1）分离法2）安全核法 安全核的设计方法：①在操作系统内核中加入安全功能 ②先设计安全核功能，然后围绕它设计操作系统3）仿真法 **6.1.4 操作系统的安全机制** I. 硬件的安全机制主要包括：内存管理、运行域保护和I/O管理。 II. 软件的安全机制主要包括：标识与鉴别机制、访问控制机制、最小特权管理机制、可信通路机制、隐通道的分析与处理以及安全审计机制等。 **1.硬件系统安全机制**1)内存保护 • 确保存储器中的数据能够被合法地访问，这种访问控制一般可以由硬件来实现。2)运行域保护 • 运行域是进程运行的区域。运行域可以看成是一系列的同心圆，最内层的特权最高，最外层的特权最低。3）I/O保护 **2.软件系统安全机制**1)标识与鉴别（认证）机制 一般可以用名称和标识符(ID)来标明系统中的一个用户。 名称和标识符可以都是公开的明码信息。鉴别是对用户身份的真实性进行识别，用于鉴别的信息一般是非公开的，并且难以伪造。2)访问控制 • 最小特权指的是在完成某种操作时授予每个主体（用户或进程）必不可少的特权。它的思想是，系统只给用户执行任务所需的最少的特权，也就是用户所得到的特权仅能完成当前任务。最小特权原则是系统安全中最基本的原则之一，它限定每个主体所必需的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小。 **审计机制** • 一个安全操作系统的审计机制就是对系统中有关安全的 活动进行记录、检查及审核。• 审计是一种被信任的机制，是TCB的一个部分。审计过程一般是一个独立的过程。**6.1.5Linux的安全机制**1.标识与鉴别机制•Linux使用用户名和户ID标识用户,使用口令来鉴别用户2.安全注意键安全注意键(SAK)是一个键或一组键(在Intelx86平台上)3.LKM机制•Linux内核是一个宏内核结构,它包括两部分:内核空间与用户空间;LKM机制,也就是可加载内核模块,简单地说就是在内核里动态载入代码的能力,LKM可以用来在运行时支持新的文件系统和设备驱动,而不用重启系统;但是,由于加载以后的LKM能够不受控制地使用内核的所有功能和内存,所以很容易引起恶意程序作为模块加入内核空间后破坏系统4.能力机制:是通过是一组比特位来实现的,该机制将root拥有的特权分割成一组特权5.日志系统•系统日志守护进程Syslogd是各类日志信息的管理者,它作为启动文件的一部分在开机后自动执行;总的来说,Linux已有的日志功能是不完善的6.防火墙机制实现了一个称为netfilter的网络层数据包过滤框架,netfilter框架为每种网络协议定义一套钩子函数,这些钩子函数在数据报流过协议栈的几个关键点被调用 **6.2 数据库安全技术 6.2.1 传统数据库安全技术** 对于数据库而言，安全性主要包括三个方面：机密性、完整性、可用性。 **数据库的安全保护需求** (1)防止不适当访问。(2)分级保护。(3)防止推断性攻击。(4)数据库的完整性。(5)数据的操作完整性。(6)数据的语义完整性。(7)审计功能。 **保证数据库管理系统安全的基本方法** 1)用户身份认证2)存取控制3)数据加密4)审计追踪与攻击检测。 **6.2.2 外包数据库安全** 外包服务把组织自己不擅长的东西（非核心业务） 交给专业的外部组织去做，将主要精力集中于核心业务。这种外包数据库运行模式带来的最大挑战就是安全问题。 • 由于数据存储在非完全可信的第三方服务器中， 因此，外包数据库系统的安全机制不但要防止来自外部的恶意攻击，而且要充分考虑来自服务 提供者本身的恶意操作。**外包数据库需采用的特定安全机制** 1．数据库加密技术由于数据库服务器非完全可信， 加密解密都应在客户端完成。2．密文数据查询策略 直接操作密文数据的应用场合包括数据库的秘密同态加密、数据库的序列加密等。分步查询是一种更具有实用价值的密文查询策略，也是目前研究的热点。这种方法一般需要进行查询分解，先对密文数据进行范围查询，缩小解密范围，快速解密后再执行精确查询。3. 数据库隐私保护 包括两个方面：1)基于推理控制的隐私内容保护2)保密信息检索 4.数据完整性验证 外包数据库系统的数据完整性要求数据库内容及其在网络中的传输具有正确性、一致性与有效性，以确保接收到的数据库内容是真实有效的，并且在传输过程中没有被攻击者插入、篡改、伪造、重排等。实现数据完整性的主要措施就是增加攻击者所不能控制的冗余信息。5．外包数据库版权保护 利用数字水印实现对外包数据库的版权保护，具有较高的研究和应用价值。 **6.2.3 云数据库/云存储安全** 云存储的定义： “云存储是通过网络提供可配置的虚拟化的存储及相关数据的服务。云存储的内涵是存储虚拟化和存储自动化。这两个定义都有几个共同的特征：首先它是基于网络的；其次它是可以配置、按需分配的；同时它是一种虚拟化的存储和数据管理。**云存储模式的安全问题** • 首先是身份认证和访问控制问题。• 第二个风险是数据存储和传输的保密性问题。• 第三是数据隔离问题。• 第四是应用安全问题。 **云存储安全机制** 云存储安全机制简单归纳为三个方面：(1)云存储平台安全机制 • 保护整个云存储平台系统自身的安全，其中主要有两个 技术：第一个是密码技术，保证完整性，提供基于PKI 的强身份鉴别以及存储节点的透明加密。另一个是加固技术，采用主动防御技术保障服务器、主机的安全性。(2)云存储管控安全机制 • 主要解决安全管理的问题，包括对云节点服务器密 钥的统一管理、密钥生命周期的可控性、云数据接口／云客户端密钥的自主性等。(3)云存储应用安全机制 • 主要从以下几方面来实现：存储加密、备份加密、交换加密、身份认证与访问控制、接口安全、手机安全以及云端数据库。 **6.3 可信计算技术** 6.3.1 概念和基本思想 可信计算是一种信息系统安全新技术。 ISO/IEC将可信定义为：参与计算的组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和一定程度的物理干扰。 • IEEE给出的可信定义为：计算机系统所提供服务的可信赖性是可论证的。 • 可信计算组织(TCG) 的定义为：一个实体是可信的，如果它的行为总是以预期的方式， 朝着预期的目标。**TCG的可信计算技术思路**：TCG的可信计算技术思路是通过在硬件平台上引入可信平台模块TPM来提高计算机系统的安全性，这种技术思路目前得到了产业界的普遍认同。**可信计算的基本思想：**可信计算的宗旨是以可信计算安全芯片为核心改进现有平台体系结构，增强通用计算平台和网络的可信性。其基本思想是：A.首先在计算机系统中建立一个信任根，信任根的可信性由物理安全、技术安全与管理安全共同确保； B. 再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用。一级测量认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。**信任的获得：**信任的获得方法主要有直接和间接两种方法。 ① 设A和B以前有过交往，则A对B的可信度可以通过考察B以往的表现来确定。称这种通过直接交往得到的信任值为直接信任值。 ② 设A和B以前没有任何交往，这种情况下，A可以 去询问一个与B比较熟悉的实体C来获得B的信任值，并且要求实体C与B有过直接的交往经验，称之为间接信任值。**6.3.2 TCG可信计算系统** 可信平台模块TPM是一种SOC芯片，它是可信计算平台的信任根。

***第七章 网络与系统攻击技术***

网络与系统攻击是利用网络与系统中存在的漏洞和缺陷实施入侵和破坏，实质上是一系列方法和手段的集合。 **7.1 网络攻击概述** 软件漏洞是软件设计或配置中能被攻击者利 用的错误或缺陷。 **7.1.1 网络攻击的概念** 定义一网络攻击是指攻击者利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行的攻击①TCP/IP协议中有很多的安全漏洞②DBMS数据的安全性、权限管理及远程访问等问题③应用设计不当，可以输入特定数据攻击。 **7.1.2 网络攻击的一般流程** (1)系统调查： • 攻击者选取攻击目标主机后，利用公开的协议或工具通过网络收集目标主机相关信息的过程。(2)系统安全缺陷探测： • 在收集到攻击目标的相关信息后，攻击者通常会利用一些自行编制或特定的软件扫描攻击目标，寻找攻击目标系统内部的安全漏洞，为实施真正的攻击做准备。步骤(1)(2)也称为网络探测。(3)实施攻击： • 当获取到足够的信息后，攻击者就可以结合自身的水平及经验总结制定出相应的攻击方法，实施真正的网络攻击。(4)巩固攻击成果： • 基于前期的侵入结果，控制目标系统，完成既定攻击任务。这一阶段的重点是长期隐蔽潜伏，并完成攻击任务。(5)痕迹清理： • 在成功实施攻击后，攻击者往往会利用获取到的目标主机的控制权，清除系统中的日志记录和留下后门，消除攻击过程的痕迹，以便日后能不被觉察地再次进入系统。 **7.2 网络探测** 网络探测也称为网络侦察。探测可以分为三个基本步骤：网络踩点、扫描和查点。网络踩点方法：①用whois通过因特网实施踩点②利用因特网搜索引擎执行踩点。**7.2.2 网络扫描** 主动式扫描和被动式扫描：主动式扫描策略是基于网络的；被动式扫描策略是基于主机的。 **常见的扫描类型** (1) TCP连接扫描(2) TCP SYN扫描（半连接扫描）(3) TCP FIN扫描(4) TCP ACK扫描(5) TCP Null扫描(6) TCP RPC扫描(7) UDP扫描(8) ICMP扫描**7.2.3常见的扫描工具**Nmap、PortScan等，知名的安全漏洞扫描工具包括开源的Nessus及商业漏洞扫描产品如ISS的Scanner系列产品 **7.3 缓冲区溢出攻击** 缓冲区溢出(buffer overflow)攻击是利用缓冲区溢出漏洞所进行的攻击行动。**7.3.1 缓冲区溢出的基本原理** 通过向目标程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达攻击目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。定义一常见的攻击方法①制造缓冲区溢出，使程序转而执行攻击者通过缓冲区溢出植入内存中的特殊指令。②如果该受到溢出攻击的程序有管理权限的话，攻击者可以很容易地获得一个有管理员权限的shell，从而实现对目标主机的控制。定义二导致缓冲区溢出漏洞的原因：①程序设计未对输入数据的合法性如长度进行认真检查②数组访问越界、序列的下标/索引越界。 **7.3.2 缓冲区溢出的防范** 对缓冲区溢出攻击的防范，目前有三种直接的保护法。 (1)通过操作系统控制使接收转入数据的缓冲区不可执行，从而阻止攻击者植入攻击代码。 (2)要求程序员编写正确的代码，包括严格检查数据、不使用存在溢出风险的函数、利用Fault injection等工具进行代码检查等。 (3)利用C编译器的边界检查来实现缓冲区的保护，这个方法使得有缓冲区溢出漏洞的进程不能被控制（劫持），但是相对而言代价比较大。 **7.4 拒绝服务攻击** 设法使目标主机停止提供服务定义一原理：利用网络协议缺陷耗尽目标主机的通信、存储或计算资源，迫使目标暂停服务甚至系统崩溃定义二可分为拒绝服务(DoS)攻击和分布式拒绝服务(DDoS)攻击。拒绝服务攻击容易引起目标警觉，只在其他方式无效时使用。**7.4.1 常见的拒绝服务攻击** 1．SYN泛洪攻击目前流行，利用TCP缺陷，发送大量伪造TCP连接请求，TCP连接无法完成第三步握手2．UDP泛洪攻击利用简单TCP/IP服务，如字符发生器协议和Echo，来传送占满带宽的垃圾数据，通过伪造与某一主机的Chargen服务之间的一次UDP连接，回复地址指向开着Echo服务的一台主机。在两台主机之间存在无用数据流，导致针对带宽服务的攻击。3．Ping泛洪攻击由于早期，路由器对包的最大尺寸都有限制，许多操作系统对TCP/IP堆栈的实现在ICMP包上都是规定64kB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区。当产生畸形时，声称自己的尺寸超过ICMP上限的包，也就是加载的尺寸超过64kB上限时，就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接收方主机宕机。4．泪滴攻击利用在TCP/IP堆栈中，实现信任IP碎片中的包的标题头所包含的信息来实现自己的攻击。IP分段含有指明该分段所包含的是原包的哪一段的信息，某些TCP/IP在收到含有重叠偏移的伪造分段时将崩溃。5．Land攻击设计一个特殊的SYN包，它的源地址和目标地址都被设置成某一个服务器地址。此举将导致接收服务器向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接。被攻击的服务器每接收一个这样的连接都将保留，直到超时。6．Smurf攻击通过向一个局域网的广播地址发出ICMP回应请求，并将返回地址设为被攻击的目标主机，导致目标主机被大量的应答包淹没，导致目标主机崩溃。不直接向目标主机发送任何数据包，而是引导大量的数据包发往目的主机，也被称为反弹攻击 **7.4.3 拒绝服务攻击的防范** 1．主机设置2．网络设备设置3． 路由器的设置(1)使用扩展访问列表(2)使用QoS(3)使用单一地址逆向转发(4)使用TCP拦截(5)使用基于内容的访问控制 **7.5 僵尸网络** 近年来，僵尸网络(BotNet)逐渐发展成为攻击者手中最有效的攻击平台，是当前互联网面临的主要安全威胁之一。 **7.5.1概念与结构** 僵尸网络是攻击者出于恶意目的，融合传统的恶意软件，如计算机病毒、蠕虫和木马等技术，传播僵尸程序传染大量主机，并通过一对多的命令与控制信道控制被感染的主机所组成的叠加网络。 包含：控制者、主机、命令与控制服务器。 **僵尸程序的典型结构**：命令与控制模块是整个僵尸程序的核心，实现了僵尸主机与控制器的交互，使将是主机接收攻击者的控制命令，进行解析和执行；传播模块通过各种不同的方式将僵尸程序传播到新的主机，使其加入僵尸网络接受攻击者的控制。信息窃取模块：用于获取感染主机信息，以及搜索并窃取感染主机上有价值的敏感信息；僵尸主机控制模块：是攻击者利用受控的大量僵尸主机完成各种不同攻击目标的模块集合；下载与更新模块：为攻击者提供向受控主机注入二次感染代码以及更新僵尸程序的功能。躲避检测与对抗分析模块：对僵尸程序进行多态、变形、加密等，并通过各种方式进行实体隐藏，以及检查debugger的存在、识别虚拟机环境、杀死反病毒进程、阻止反病毒软件升级等功能，使得僵尸程序能够躲避受控主机使用者和反病毒软件的检测。 **7.5.2 工作机制** (1)感染目标主机，构建僵尸网络(2)发布命令，控制僵尸程序。(3)展开攻击。(4)攻击善后。**7.6 缓冲区溢出漏洞的分析与利用** 由于函数里局部变量的内存分配是发生在栈帧里的，所以如果在某一个函数内部定义了缓冲区变量，则这个缓冲区变量所占用的内存空间是在该函数被调用时所建立的栈帧里。 • 由于对缓冲区的潜在操作(比如字串的复制)都是从内存低址到高址的，而内存中所保存的函数返回地址往往就在该缓冲区的上方(高地址)——这是由于栈的特性决定的，这就为覆盖函数的返回地址提供了条件。 • 当用大于目标缓冲区大小的内容来填充缓冲区时，就可以改写保存在函数栈帧中的返回地址，从而改变程序的执行流程，执行攻击者的代码。

**7.6.2 缓冲区溢出攻击技术** 方法一：将Shellcode放置在跳转地址(函数返回地址所在的栈)之前如果被攻击的缓冲区较大，足以容纳Shellcode，则可以采用这种方法方法二：将Shellcode放置在跳转地址(函数返回地址所在的栈)之后，如果被攻击的缓冲区的长度小于Shellcode的长度，不足以容纳shellcode，则只能将Shellcode放置在跳转地址之后

在漏洞函数的3个地方设置断点： • (1) 第一条汇编语句：在此记下函数的返回地址 （A=esp的值） (动态变化) • (2) 调用strcpy对应的汇编语句：记下smallbuf的起始 地址=$esp=B (动态变化)，与A相减可以得到产生缓 冲区溢出所需的字节数Offset=A-B • (3) ret语句：查看esp的内容，确定被修改的返回地址。

**Hw attack\_overflow.c中的foo函数buff[16]改为buff[123] 堆栈距离Offset为:0xbffff02c-0xbfffefa5=28+(123-16)=135**

***第八章 网络与系统安全防护***

安全防护是指为保护己方网络和系统正常工作，保护信息数据安全而采取的措施和行动。 • 攻击和防护是矛和盾的关系。在建立安全防护体系时，必须走管理和技术相结合的道路。安全防护的涉及面很宽，从技术层面上讲主要包括防火墙技术、入侵检测技术、 “蜜罐”技术、 应急响应技术。 • 此外，从广义上看，病毒防护技术、数据加密技术和认证技术也属于安全防护技术。**8.1 防火墙技术** 防火墙的定义：防火墙是位于两个(或多个)网络之间执行访问控制的软件和硬件系统，它根据访问控制规则对进出网络的数据流进行过滤。 **8.1.1 防火墙的概念** 在计算机网络安全领域，防火墙是一个由软件和硬件组合而成的、起过滤和封锁作用的计算机系统或者网络系统，它一般部署在本地网络和外部网之间，内部网络被 认为是安全和可信赖的，外部网络则是不安全和不可信赖的。 • 防火墙的作用是隔离风险区域（外部网络）与安全区域（内部网）的连接，阻止不希望的或者未授权的通信进出内部网络，通过边界控制强化内部网络的安全，同时不会妨碍内部网对外部网络的访问。 **防火墙的概念** 网络防火墙隔离了内部网络和外部网络，在企业内部网和外部网(Internet)之间执行访问控制策略，以防止发生不可预测的、外界对内部网资源的非法访问或潜在的破坏性侵入。 **8.1.2 防火墙的特性** 防火墙的设计目标：(1)针对所有的通信，无论是从内部到外部还是从外部到内部的，都必须经过防火墙。这一点可以通过阻塞所有未通过防火墙的对本地网络的访问来实现。 (2)只有被授权的通信才能通过防火墙，这些授权将在安全策略中规定。不同类型的防火墙实现不同的安全策略。 (3)防火墙本身对于渗透攻击必须是免疫的。这意味着必须使用运行安全操作系统的可信系统。 **防火墙采用的4项常用技术** (1) 服务控制(2) 方向控制(3) 用户控制(4) 行为控制 **防火墙具有的典型功能** (1)访问控制功能(2)内容控制功能(3)日志功能(4)集中管理功能(5)自身安全和可用性 **防火墙的局限性** (1)防火墙不能防御不经由防火墙的攻击。 (2)防火墙不能防范来自内部的威胁。 (3)防火墙不能防止病毒感染的程序和文件进出内部网。 (4)防火墙不能防止数据驱动式的攻击。 8.1.3 防火墙的技术 根据不同的分类标准，可将防火墙分为不同的类型。 A. 从工作原理角度看，防火墙技术主要可分为网络层防火墙技术和应用层防火墙技术。 B. 根据实现防火墙的硬件环境不同，可将防火墙分为基于路由器的防火墙和基于主机系统的防火墙。。 C. 根据防火墙的功能不同，可将防火墙分为FTP防火墙、Telnet防火墙、E-mail防火墙、病毒防火墙、个人防火墙等各种专用防火墙。**1 包过滤技术** 网络层技术的一个范例就是包过滤技术。 1）包过滤原理包过滤技术是最早的防火墙技术，工作在网络层。 • 这种防火墙的原理是将IP数据报的各种包头信息与防火墙内的规则进行比较，然后根据过滤规则有选择地阻止或允许数据包通过防火墙。常用的包头信息包括源地址、目的地址、源端口、目的端口、协议类型等。 **包过滤防火墙的主要工作原理** 包过滤防火墙要遵循的一条基本原则就是“最小特权原则” ，即明确允许管理员希望通过的那些数据包，禁止 其他的数据包。包过滤的核心技术是安全策略及过滤规则的设计。 **包过滤防火墙的具体实现** 1. 建立安全策略，写出所允许和禁止的任务，将安全策略转化为一个包过滤规则表。2. 由规则表和数据头内容的匹配情况来执行过滤操作默认的策略可能是： ① 默认值：丢弃。② 默认值：转发。 **包过滤防火墙的优点：** (1) 一个过滤器能协助保护整个网络。 (2)包过滤用户对用户透明。 (3)过滤路由器速度快、效率高。 (4)技术通用、廉价、有效。 • 此外，包过滤防火墙还易于安装、使用和维护。 **包过滤防火墙的缺点：**(1)安全性较差。 (2)由于防火墙可用的信息有限，它所提供的日志功能也十分有限。 (3)无法执行某些安全策略。 (4)这种防火墙通常容易受到利用TCP/IP规定和协议栈漏洞的攻击，例如网络层地址欺骗。 (5)在这种防火墙做出安全控制决定时，起作用的只是少数几个因素，包过滤器防火墙对由于不恰当的设置而导致的安全威胁显得十分脆弱。 **代理服务技术 代理服务技术原理** 代理服务器防火墙又称应用层网关、应用层防火墙，它工作在OSI模型的应用层，掌握着应用系统中可用作安全决策的全部信息。 • 代理服务技术的核心是运行于防火墙主机上的代理服务器程序，这些代理服务器程序直接对特定的应用层进行服务。 • 代理服务器防火墙完全阻隔了网络通信流，通过对每种应用服务编制专门的代理服务程序，实现监视和控制应用层通信流的作用。 **代理服务器的实现** (1)应用代理服务器 • 应用代理服务器可以在网络应用层提供授权检查及代理服务功能。当外部某台主机试图访问受保护的内部网时， 它必须先在防火墙上经过身份认证。(2)回路级代理服务器 • 回路级代理服务器也称一般代理服务器，它适用于多个协议，但不解释应用协议中的命令就建立连接回路。回路级代理服务器通常要求修改过的用户程序。(3)智能代理服务器(4)邮件转发服务器 **代理服务器防火墙的特点** (1)安全性好。安全性好是代理服务技术突出的特点。 (2)易于配置。 (3)能生成各项记录。代理生成的日志和记录对于流量分析、安全检验是十分重要的。 (4)能完全控制进出的流量和内容。 (5)能过滤数据内容。 可以把一些过滤规则应用于代理，让它在高层实现过滤功能，例如，文本过滤、图像过滤、预防病毒和扫描病毒等。 (6)能为用户提供透明的加密机制。 (7)可以方便地与其他安全技术合成。 **代理服务技术的缺点** (1)速度较慢。 (2)对用户不透明。 (3)对于不同服务器代理可能要求不同的服务器，可能需要为每项协议设置一个不同的代理服务器。(4)通常要求对客户或者过程进行限制。(5)代理不能改进底层协议的安全性。 **状态检测技术 1）状态检测技术的工作原理** 状态检测技术由CheckPoint率先提出，又称动态包过滤技术。 • 状态检测技术是一项新的防火墙技术。这种技术具有非常好的安全特性，它使用一个在网关上实行的网络安全策略的软件模块，称为检测引擎。 • 检测引擎在不影响网络正常运行的前提下，采取抽取有关数据的方法对网络通信各层实时监测。检测引擎将抽取的状态信息动态地保存起来作为以后执行安全策略的参考。• 检测引擎维护一个动态的状态信息表并对后续的数据包进行检查，一旦发现任何连接的参数有意外的变化，连接就被终止。状态检测技术监视和跟踪每一个有效连接的状态，并根据这些信息决定网络数据包是否能通过防火墙。**通过状态检测防火墙数据包的类型** (1)TCP包 (2)UDP包 **状态检测技术的特点和应用** 状态检测技术结合了包过滤技术和代理服务技术的特点。 • 状态检测技术克服了包过滤技术和代理服务技术的局限性，能根据协议、端口及源地址、目的地址的具体情况决定数据包是否通过。 • 状态检测技术的缺点是状态检测可能造成网络连接的某种迟滞，但运行速度越快，这个问题就越不易察觉。 **8.1.4 自适应代理技术** 自适应代理防火墙技术，本质上也属于代理服务技术，但它也结合了动态包过滤（状态检测）技术。自适应代理防火墙结合了代理服务器防火墙的安全性和包过滤防火墙的高速等优点，在保证安全性的基础上将代理服务器防火墙的性能提高十倍以上。 **8.1.5 防火墙的体系结构** 1)屏蔽主机防火墙（单宿堡垒主机）2)屏蔽主机防火墙（双宿堡垒主机）**单宿堡垒主机体系缺陷** 在单宿堡垒主机体系中，如果包过滤路由器被攻破，那么通信就可以越过路由器在Internet和内部网络的其他主机之间直接进行。• 屏蔽主机防火墙双宿堡垒主机结构在物理上防止了这种安全漏洞的产生(图8-3(b))。双宿堡垒主机具有至少两个网络接口，外部网络和内部网络都能与堡垒主机通信，但是不能直接通信，它们之间的通信必须经过双宿堡垒主机的过滤和控制。 3)屏蔽子网防火墙 **8.1.6 防火墙的应用与发展 1. 防火墙的应用** 选用防火墙首先要明确哪些数据是必须保护的，这些数据的被侵入会导致什么样的后果，以及网络不同区域需要什么等级的安全级别。选用防火墙时要注意防火墙自身的安全性。 **防火墙的选用** 防火墙的选用也要考虑用户的安全策略中的特殊需求，比如： (1) IP地址转换 (2)双重DNS (3)虚拟专用网络(VPN) (4)病毒扫描功能 (5)特殊控制需求。 **防火墙技术的发展** 1)智能化 2)高速度 3)分布式并行结构 4)多功能 5)专业化 **未来防火墙的发展思路** ① 防火墙将从目前对子网或内部网管理的方式向远程上网集中管理方式发展；过滤深度不断加强，并逐渐有病毒清除功能。 ② 利用防火墙建立VPN是较长一段时间内用户使用的主流；对网络攻击的检测和告警将成为防火墙的重要功能。 ③ 此外，网络的防火墙产品还将把网络前沿技术，如Web页面超高速缓存、虚拟网络和带宽管理等与其自身结合起来。 **8.2 入侵检测技术** 传统的安全防护技术包括防火墙、杀毒软件、加密软件等，也称为“被动防护”技术，难于及 时应对日趋复杂多样的攻击工具与手法带来的挑战。 • 入侵检测是一种从更深层次上进行“主动”网络安全防御的措施。具有主动性和实时性的特点。 **8.2.1 入侵检测概述 1.入侵检测的概念** 入侵检测是指在计算机网络或计算机系统中的若干关键点收集信息并对收集到的信息进行分析， 从而判断网络或系统中是否有违反安全策略的行为和被攻击的迹象。它是对入侵行为的发觉。 • 入侵检测作为安全技术，其主要目的在于： • 第一，识别入侵者； • 第二，识别入侵行为； • 第三，检测和监视已成功的安全突破； • 第四，为对抗入侵及时提供重要信息，阻止事件的发生和事态的扩大。入侵就是试图破坏网络及信息系统机密性、完整性和可用性等安全属性的行为。入侵方式一般有： (1)未授权的用户访问系统资源； (2)已经授权的用户企图获得更高权限，或者是已经授权的用户滥用所给定的权限等。 • 入侵检测的概念：入侵检测是监测计算机网络和系统、发现违反安全策略事件的过程。 入侵检测的定义：入侵检测是对企图入侵、正在进行的入侵或已经发生的入侵行为进行识别的过程。 **入侵检测过程** 入侵检测的典型过程是：信息收集、信息（数据）预处理、数据的检测分析、根据安全策略做出响应。有的还包括检测效果的评估。 ① 信息收集是指从网络或系统的关键点得到原始数据，这里的数据包括原始的网络数据包、系统的审计日志、应用程序日志等原始信息； ② 数据预处理是指对收集到的数据进行预处理，将其转化为检测器所需要的格式，也包括对冗余信息的去除，即数据简约； ③ 数据的检测分析是指利用各种算法建立检测器模型，并对输入的数据进行分析以判断入侵行为的发生与否。 入侵检测的效果如何将直接取决于检测算法的好坏。 ④ 响应是指产生检测报告，通知管理员，断开网络连接，或更改防火墙的配置等积极的防御措施。 **审计记录的两种方法：**(1)原始审计记录 (2)检测专用审计记录 **每个审计记录包含的域** (1)主体：行为的发起者。(2)动作：主体对一个对象的操作或联合一个对象完成的操作。(3)客体：行为的接收者。(4)异常条件(5)资源使用(6)时间戳。 **3 入侵监测系统** 入侵检测系统是完成入侵检测功能的软件、硬件的组合。IETF定义了一个IDS的通用入侵检测模型（CIDF）包含如下物件：(1)事件生成器：它是采集和过滤事件数据的程序或模块。(2)事件分析器：事件分析器是分析事件数据和任何CIDF组 件传送给它的各种数据。(3)事件数据库：负责存放各种原始数据或已加工过的数据。(4)响应单元：是针对分析组件所产生的分析结果，根据响 应策略采取相应的行为，发出命令响应攻击。(5)目录服务器：目录服务器用于各组件定位其他组件，以及控制其他组件传递的数据并认证其他组件的使用，以防止入侵检测系统本身受到攻击。**入侵检测系统的主要功能** (1)监测并分析用户和系统的活动。 (2)核查系统配置与漏洞。 (3)识别已知的攻击行为并报警。 (4)统计并分析异常行为。 (5)对操作系统进行日志管理，并识别违反安全策略的用户活动。 **8.2.2 入侵检测系统分类 1.基于检测对象的分类 1)基于主机的入侵检测系统** • (host-based IDS，HIDS)开始并兴盛于20世纪80年代， 其检测对象是主机系统和本地用户。**1)基于主机的入侵检测系统的优缺点 优点：**(1)能确定攻击是否成功。(2)监控更为细致。(3)配置灵活。(4)适应于加密和交换的环境。(5)对网络流量不敏感。**缺点**：(1)由于它通常作为用户进程运行，依赖于操作系统底层的支持， 与系统的体系结构有关，所以它无法了解发生在下层协议的入侵活动。 (2)由于HIDS要驻留在受控主机中， 对整个网络的拓扑结构认识有限，根本监测不到网络上的情况，只能为单机提供安全防护。 (3)基于主机的入侵检测系统必须配置在每一台需要保护的主机上，占用一定的主机资源，使服务器产生额外的开销。 (4)缺乏对平台的支持，可移植性差。**2)基于网络的入侵检测系统（NIDS）** 基于网络的入侵检测系统通过监听网络中的分组数据包来获得分析攻击的数据源，分析可疑现象。**1)基于网络的入侵检测系统的优缺点 优点：**1)监测速度快。(2)能够检测到HIDS无法检测的 入侵。(3)入侵对象不容易销毁证据。(4)检测和响应的实时性强。(5)与操作系统无关性。缺点：(2)能够检测到HIDS无法检测的入侵。 (3)入侵对象不容易销毁证据。 被截取的数据不仅包括入侵的方法，还包括可以定位入侵对象的信息。 (4)检测和响应的实时性强。一旦发现入侵行为就立即终止攻击。 (5)与操作系统无关性。由于基于网络的IDS是配置在网络上对资源进行安全监控，因此， 它具有与操作系统无关的特性。 **缺点：** (1) NIDS无法采集高速网络中的所有数据包。NIDS难以检测发生在应用层的攻击。(3) NIDS对以加密传输方式进行的入侵无能为力。(4) NIDS只检查它直接连接网段的通信，并且精确度较差，在交换式网络环境下难以配置，防入侵欺骗的能力较差。**3)混合式入侵检测系统** 综合了网络和主机两种结构特点的IDS，既可以发现网络中的攻击信息，也可以从系统日志中发现异常状况，这就是混合式入侵检测系统。 **2.基于检测技术的分类** 根据入侵检测技术，可分为异常检测和误用检测两类。**1)异常检测** • 异常检测也称之为基于行为的检测，来源于这样的思想：任何一种入侵行为都能由于其偏离 正常或者所期望的系统和用户的活动规律而被检测出来。 **优缺点：优点是：** • 第一，正常使用行为是被准确定义的，检测的准确率高； • 第二，能够发现任何企图发掘、试探系统最新和未知漏洞的行为，同时在某种程度上，它较少依赖于特定的操作系统环境。**缺点是**： • 第一，必须枚举所有的正常使用规则，否则会导致有些正常使用的行为会被误认为是入侵行为，即有误报产生； • 第二，在检测时，某个行为是否属于正常，通常不能做简单的匹配，而要利用统计方法进行模糊匹配，在实现上有一定的难度。 **2)误用检测** 误用检测又称之为特征检测，建立在对过去各种已知网络入侵方法和系统缺陷知识的积累之上。误用检测是直接对入侵行为进行特征化描述，其主要优点有：依据具体特征库进行判断，检测过程简单，检测效率高，针对已知入侵的检测精度高，可以依据检测到的不同攻击类型采取不同的措施。 • 缺点有：对具体系统依赖性太强，可移植性较差，维护工作量大，同时无法检测到未知的攻击。 **3.基于工作方式的分类** 根据工作方式，可分为离线检测系统和在线检测系统。 1)离线检测系统 • 离线检测系统是非实时工作的系统，它在事后分析审计事件，从中检查入侵活动。• 在线检测系统是实时联机的检测系统，它包含对实时网络数据包分析和实时主机审计分析。 **8.2.3 分布式入侵检测** 分布式入侵检测系统的各个模块分布在网络中 不同的计算机设备上。 • 一般来说，分布性主要体现在数据收集模块上，如果网络环境比较复杂、数据量比较大，那么数 据分析模块也会分布在网络的不同计算机设备 上，通常是按照层次性的原则进行组织。 • 分布式入侵检测系统根据各组件间的关系还可细 分为层次式DIDS和协作式DIDS。 **典型分布式入侵检测系统结构** (1)主机代理模块 (2) 局域网监视代理模块 (3)中心管理员模块 **8.2.4 入侵检测技术发展趋势** 入侵检测系统目前主要存在以下几个问题： (1)高速网络下的误报率和漏报率 (2)入侵检测产品和其他网络安全产品结合的问题 (3)入侵检测系统的功能相对单一 (4)入侵检测系统本身存在的问题。 **入侵检测的研究重点** (1) 分布式入侵检测(2) 智能入侵检测(3) 高效的模式匹配算法(4) 基于协议分析的入侵检测(5) 与操作系统的结合(6) 入侵检测系统之间以及入侵检测系统和其他安 全组件之间的互动性研究(7) 入侵检测系统自身安全性的研究(8) 入侵检测系统的标准化 **8.3 “蜜罐”技术 8.3.1 蜜罐的概念** 蜜罐是防御方为了改变网络攻防博弈不对称局面而引入的一种主动防御技术，本质上是一种没有任何产品价值的安全资源，其价值体现在被探测、攻击或者攻陷的时候。 • 蜜罐技术是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息（蜜罐），诱使攻击方对它们实施攻击，从而可以对攻行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。 **蜜网** 蜜网(honeynet)又可称为诱捕网络，是由若干个能收集和交换信息的蜜罐构成的一个网络体系架构。 **8.3.2 蜜罐技术的分类** 1．按系统功能分类 • 产品型蜜罐和研究型蜜罐两类。 2．按系统交互活动级别分类 • 根据系统允许与黑客交互活动的级别，蜜罐可分为低交互蜜罐与高交互蜜罐。 3．按服务实现方式分类 • 为了欺骗攻击者，蜜罐需要提供与真实的主机相似的操作系统和服务。根据服务实现方式将蜜罐系统分为真实蜜罐和虚拟蜜罐。 4．按服务提供方式分类 • 根据服务提供方式将蜜罐分为服务端蜜罐和客户端蜜罐。 **8.3.3 蜜罐技术关键机制** 蜜罐技术的核心机制是蜜罐技术达成对攻击方进行诱骗与监测的必需组件，包括： (1) 欺骗环境构建机制 • 构造出对攻击方具有诱骗性的安全资源，吸引攻击方对其进行探测、攻击与利用。 (2) 威胁数据捕获机制 • 对诱捕到的安全威胁进行日志记录，尽可能全面地获 取各种类型的安全威胁原始数据，如网络连接记录、 原始数据包、系统行为数据、恶代码样本等。 (3) 威胁数据分析机制 • 在捕获的安全威胁原始数据的基础上，分析追溯安全 威胁的类型与根源，并对安全威胁态势进行感知。 **蜜罐技术的辅助机制** (1) 安全风险控制机制(2) 配置与管理机制(3) 反蜜罐技术的对抗机制

1. ***安全审计与责任认定技术***

**8.4 应急响应技术 8.4.1 应急响应的概念 需要应急响应的原因：**网络与信息系统面临诸多威胁，安全防护技术 不能保证系统100%的安全。 **什么是应急响应** 应急响应就是对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策， 保证计算机信息系统和网络免遭破坏。 **CSIRT的类型** (1)内部CSIRT(2)国家CSIRT(3)协调中心CC(4)分析中心AC(5)卖方团队(6)应急响应提供商 **8.4.2 应急响应策略** 按照策略的作用范围，可以分为如下几种：① 全局策略 ② 服务特定策略 ③ 基础策略 **8.4.3 应急事件处理流程** CSIRT主要提供以下服务：1）安全事件的热线响应 包括：(1)检查入侵来源(2)恢复系统正常工作(3)事故分析(4)发布安全警报、安全公告、安全建 议(5)咨询(6)风险评估(7)安全教育培训(8)协助其他组织成立自己的CSIRT， 建立网络应急与救援队伍。2）应急响应的主要阶段 (1)准备阶段：准备阶段的主要工作包括建立合理的防御／控制措施、建立适当的策略和程序、获得必要的资源和组建响应队伍等。(2)检测阶段：检测阶段要做出初步的动作和响应。根据获得的初步材料和分析结果，估计事件的范围和发展势态，制定进一步的响应战略，并且保留可能用于司法程序的证据。(3)抑制阶段：抑制的目的是限制攻击的范围。(4)根除阶段在事件被抑制之后，通过对有关恶意代码或行为的分析结果，找出事件根源并彻底清除。(5)恢复阶段恢复阶段的目标是把所有被攻破的系统和网络设备彻底还原到它们正常的运行状态。(6)报告和追踪阶段。• 这个阶段的目标是回顾并整理发生事件的各种相关信息，尽可能地把所有情况记录到文档中。**8.4.4 应急响应技术及工具** 1)应急响应技术 应急响应的技术包括漏洞检测技术、监听技术、日志分析技术、路由控制技术、反向追踪技术等。2)支持CSIRT日常运作的工具和技术 (1)执行CSIRT运作流程：事件跟踪和报告；事件分类和归档；通信。 • (2)提供安全远程访问：远程网络访问；远程拨号访问；安全隧道。 • (3)前置工具，支持审计／检测漏洞／预防事件：网络审计；主机审计；软件审计；网络监控；网络入侵检测。3)支持事件调查的工具 (1)证据收集工具：检查存储媒体；检查系统。 (2)证据调查工具：分析证据；校验同一性。 **9.1 安全审计 9.1.1 安全审计概念** 所谓审计，简单地说就是记录和分析用户使用信息系统过程中的相关事件。 • 不仅记录谁访问了系统，而且记录系统以何种方式被使用。 • 基于对记录的系统事件的分析，能够快速地识别问题，确定是否有攻击、攻击源自何处。因此，审计本质上是一种为事后观察、分析提供支持的机制，广泛存在于信息系统中，记录、分析、报告系统中的事件。 • 安全审计则是对系统安全的审核、稽查与计算，即在记录一切或部分与系统安全有关活动的基础上，对其进行分析处理、评价审查，发现系统中的安全隐患，或追查出造成安全事故的原因，并做出进一步的处理。 **安全审计及主要功能** 安全审计除了能够监控来自信息系统内部和外部 的用户活动，对与安全有关的活动的相关信息进行识别、记录、存储和分析，对突发事件进行报警和响应，还能通过对系统事件的记录，为事后处理提供重要依据，为网络犯罪行为及泄密行为提供取证基础。同时，通过对安全事件的不断积累并且加以分析，能有选择性和针对性地对其中的对象进行审计跟踪，即事后分析及追查取证，以保证系统的安全。 1)安全审计自动响应 2)安全审计数据生成 3)安全审计分析 4)安全审计浏览 5)安全审计事件存储 审计系统在审计事件存储方面遇到的问题通常是磁盘空间用尽。6)安全审计事件选择 **9.1.2 审计系统的结构** 1.集中式结构 2.分布式结构 (1)主机代理模块 (2)局域网监视器代理模块 (3)中央管理者模块 **分布式系统结构的工作过程** 工作过程 ① 主机代理模块截获审计收集系统生成的审计记录然后将这些记录转化成一种标准格式以实现互操作。 ② 局域网监视器代理审计主机与主机之间的连接以及使用的服务和通信量的大小，以查出显著的事件。 **分布式系统结构的优点** (1)扩展能力强(2)容错能力强(3)兼容性强(4)适应性强 **在设计分布式系统要考虑以下几个主要问题** (1)需要处理不同的格式以实现不同节点间互操作。（2）原始的审计数据或者总结数据必须通过网络进行传输，因而存在保证这些数据完整性和机密性的需求。分析中心设置问题：可以采用集中或分散的结构。**9.1.3 审计的数据来源** 网络安全审计系统的数据采集的完整性和准确性是其后续分析和处理的基础，其数据源可以分为三类：基于主机、基于网络和其他途径。 **1. 基于主机的数据源** 1)操作系统日志 • 操作系统日志主要由三个元素来描述，主体 (subject)、客体(object)和行为(action)。它从三个方面收集系统事件：操作系统事件、 安全事件和应用程序事件。操作系统日志是基于主机的审计系统或入侵检测系统的首选数据源。2)系统日志3)应用日志4)基于目标的信息：有时，人们希望只对系统的部分活动或部分资源进行审计，由此产生了面向目标的安全审计。最常见的基于目标的审计技术是完整性校验。 **2. 基于网络的数据源 基本原理** 1)网络数据的获取 • 以太网网络适配器（网卡）通常有正常模式和混杂模式。基于网络的安全审计系统必须利用网络适配器的混杂模式，获得经过本网段的所有数据信息，从而实现获取网络数据的功能。 2）采用网络数据源的优势 (1)由于网络嗅探器(sniffer)所做的工作仅仅是从网络中读取传输的数据帧，因此，对受保护系统的性能影响很小或几乎没有，并且无须改动原先的系统和网络结构。 (2)网络嗅探器对网络中的用户是透明的，降低了嗅探器本身遭受入侵者攻击的可能性。 (3)网络监听相对于基于主机的安全审计，更容易检测到某些基于网络协议的攻击方法。(4)网络监听可针对一个网络的数据进行分析，与受保护主机的操作系统无关。 **3. 其他途径的数据源** 路由器、交换机等网络设备产生的活动日志，以及带外数据源。 **9.2 数字取证 9.2.1 数字取证概述** 数字取证(以下简称取证)，也被称为计算机及网络取证、计算机取证 ，就是应用计算机、通信等相关技术，发现、收集、检查、分析数据，同时保护信息的完整性，并维持严格的数据保管链。数字取证的作用，就是通过调查可疑的计算机和网络系统，收集和保存证据，重建事件，评估事件的状态，获得证据，从而进行犯罪调查或者响应一个计算机安全紧急事件。数字取证的作用包含以下几点：获得证据，打击违法犯罪(主要作用)。其他作用：（1）排除故障（2）日志监控（3）数据恢复（4）数据提取（5）完善策略。数字取证的分类：（1）主机取证和网络取证（2）事后取证和实时取证（3）司法取证和非司法取证。数字取证的数据媒介：① 标准的计算机系统② 网络设备③ 外部设备④ 存储设备⑤ 消费电子产品 **9.2.2 电子证据的特点和取证基本原则** 取证的直接目的：得到说明或验证某个事件的证据。 • 计算机取证得到的证据称为电子证据或数字证据。电子证据必须满足两个根本属性。 ① 可接受性：在技术上或者法律上可以接受。 ② 完整性：数据是真实、可靠的。 • 真实性是指数据来源于它本来的地方并且没有被污染； • 可靠性指的是数据所说明的事实是可信的和一致的，需要将数据与其结果关联。**电子证据的特点** (1)数字型(2)技术性(3)脆弱性 计算机系统对数据的处理环节多、使用的技术和设备复杂、处理速度越来越快，数据的修改可以在瞬间完成，并且可以不留痕迹，从而使得电子证据具有脆弱和不可靠的特性。(4)多态性 • 是指电子证据的表现形式是多种多样的，即不同形态输出材料的证明力都来源于同一计算机存储的信息本身。(5)人机交互性 • 是指电子证据的形成，在不同的环节上有不同计算机操作人员的参与，并且会对电子证据施加不同的影响，这种影响的层次和程度与操作人员的工作性质有关。(6)复合性 • 当证据以某种形式表现时，往往就具有了这种表现形式的证据特征。电子证据是多种形式证据的集合。 **计算机取证应该遵循的原则** (1)及时性原则：要求计算机证据的获取有一定的时效性。 (2)取证过程合法性原则： • 要求计算机取证过程必须按照法律的规定公开进行，得到第一手具有证明力的公正的证据信息。 (3)多备份原则： • 对于含有电子证据的媒介至少应制作两个副本，原始媒介应妥善保管，副本用于取证人员进行证据的提取和分析。 (4)环境安全原则： • 取证过程应该在安全环境中进行，以各随时重组、试验或展示。存储证据 的媒介应远离高磁场、高温、灰尘、积压、潮湿、腐蚀性化学试剂等。(5)严格管理过程的原则： • 含有计算机证据媒介的移交、保管、开封、拆卸的过程必须由应急响应取证人员和保管人员共同完成，每一个环节都必须检查其真实性和完整性， 并拍照和制作详细的笔录，由行为人共同签名，从而形成完整的证据链。**9.2.3 数字取证的过程** 收集->检查->分析->报告 写报告要考虑:(1)不同的解释(2)不同的听众 **9.3 数字取证的关键技术和工具 9.3.2 来自文件的数字取证技术** 除了标准的文件，还有一些特殊数据，它们在取证中有时也可以起到极为重要的作用。 (1)删除的文件(2)松弛空间(slack space)(3)空闲区**1.收集文件**：1)从媒介复制文件 取证工作应该在工作拷贝上进行。1)从媒介复制文件。有两种技术用来从媒介复制文件：(1)逻辑备份(2)比特流映像。执行逻辑备份时，要注意在复制过程中文件会变化，而且被一个进程打开的文件不容易复制。 **1．收集文件**：2)数据文件完整性3)文件的MAC属性 UNIX维护着文件的三个时间戳，也称MAC times，记录最后修改时间、最后访问时间、最后状态改变时间等信息。如果要建立整个事件发生的精确的时间戳(timeline)，就必须妥善保护好时间属性。**1．收集文件**：4)其他技术问题 （1）数据恢复（2）隐含数据的恢复（3）RAID阵列数据的收集（4）关于数据编码和解码 **2.检查数据文件：**1)定位文件2）提取数据3）使用取证工具进行检测 **3.分析文件 9.3.3 来自操作系统的数据取证技术 1.收集操作系统数据** 1)收集易失性数据2)收集非易失性数据