信息安全导论小抄郭箪霄 PB20111712 一、绪论信息已成为一种重要的战略资源。习近平指出：没有网络安全就没有国家安全。1.1 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（消息层次）机密性、完整性、不可抵赖性、（网络层次）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。信息安全属性 1 机密性：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：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：确保实体就是所声称的实体。标识和认证。4 不可否认性：审计和日志，数字签名和安全协议。5 可靠性。6 可用性：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：访问控制。8 保鲜性（新鲜性）：信息必须是在其时效之内的。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。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。1 信息泄露。2 非授权的篡改。3 拒绝服务。4 非法使用（非授权访问）。5 假冒。6 抵赖。7 网络与系统攻击。8 恶意代码。9 自然灾害。10 人为失误和故意破坏。安全威胁分别破坏不同的信息安全属性。安全是相对的，不安全才是绝对的。过时的"成功"和"赔本"的攻击都被认为是无效的。1.2 信息安全发展历程：第一时期：通信安全时期这个时期的安全性是指信息的保密性，对安全理论和技术的研究也仅限于密码学。这一阶段的信息安全技术可以简称为通信安全，关注如何保证数据在从一地传送到另一地时的安全性。第二个时期：计算机安全时期人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段。数据加密标准（DES）和可信计算机系统评估准则标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。第三个时期：网络安全时代信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为可控性、抗抵赖性、真实性等其他的原则和目标。第四个时期：信息安全保障时代其主要标志是《信息保障技术框架》（IATF）。面向业务的安全保障：体系性的安全保障。深度防御体系。从整体角度考虑其体系建设的信息安全保障时代。1.3 信息安全技术体系 1 核心基础安全技术（密码技术（密码算法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。密码分析技术破解密码算法或密码协议）、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。隐写。数字水印。数据隐藏））2 安全基础设施技术（标识与认证技术（标识是指实体的表示。认证技术就是鉴别实体身份的技术）、授权与访问控制技术（给已通过认证的用户授予相应的操作权限））3 基础设施安全技术（主机系统安全技术（主机系统主要包括操作系统和数据库系统等。可信计算）、网络系统安全技术（传输层安全的 SSL/TLS，网络层安全的 IPSec，应用层安全的安全电子交易 SET））4 应用安全技术（网络与系统攻击技术（攻击者利用信息系统弱点（漏洞）破坏或非授权地侵入网络和系统。包括网络与系统调查、口令攻击、拒绝服务攻击（DoS）、缓冲区溢出攻击）、网络与系统安全防护与应急响应技术（抵御网络与系统遭受攻击。主要包括防火墙和入侵检测技术。入侵检测系统（IDS）。蜜罐。应急响应技术）、安全审计与责任认定技术、（相应事件的调查方法与取证手段）恶意代码检测与防范技术（防范技术需要利用恶意代码的不同特征来检测并阻止其运行。僵尸网络。僵尸程序）、内容安全技术（监控数字内容传播））5 支撑安全技术（信息安全保障技术框架（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。由保护网络与基础设施、保护区域边界和外部连接、保护计算环境及支持性基础设施这四个框架域所共同组成）、信息安全测评与管理技术（对信息安全产品或信息系统的安全性等进行验证、测试、评价和定级。涉及安全管理制度的制定、物理安全管理、系统与网络安全管理、信息安全等级保护及信息资产的风险管理等内容））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，是信息系统在何种环境下遭受威胁并获得信息安全的一般性描述。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：被密码协议的设计者广泛采用。为了抵抗主动攻击，必须有一种机制识别信息的篡改，这就是数字签名技术。为了抵抗被动攻击，密码算法必须在计算上是安全的，同时对加密后的信息必须进行重组，以抵抗统计分析。永远不能低估攻击者的知识和能力。1.5 信息安全保障技术 IATF 的焦点框架区域划分网络和基础设施、区域边界、计算环境和支撑性基础设施。IATF 的核心思想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。全方位、多层次。人、技术和操作是三个主要核心要素。IATF 的其他信息安全原则保护多个位置、分层防御、安全强健性（即强度和保障。信息价值和安全管理成本）。框架世界各主要强国都将网络空间安全提升到国家战略的高度。《网络空间安全战略》指出，"网络空间的国际竞争方兴未艾"是我国网络空间安全面临的重大挑战之一。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。进攻是最好的防守。二、密码技术 2.1 基本概念密码学=密码编码学+密码分析学。明文：原始的消息。密文：加密后的消息。密码学模型一般意义上的 Password≠Key，Password（口令）是一串字符，Key（密钥）是加密/解密过程中的参数。密码体制五元组（P,C,K,E,D）。P 称为明文空间；C 称为密文空间；K 称为密钥空间；E 和 D 分别表示加密算法和解密算法的集合，$d_k(e_k(m))=m$。对称密码体制也叫单钥密码体制或秘密密钥密码体制。非对称密码体制也称为公钥（公开密钥）密码体制。公钥,通常用于加密。私钥通常用于解密。密码体制的安全性无条件安全、计算上安全（(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密码分析攻击（企图利用算法的特征来恢复出明文，或者推导出使用的密钥。唯密文攻击、已知明文攻击选择明文攻击、选择密文攻击）、穷举攻击（对所有可能的密钥组合进行测试。要获得成功必须尝试所有可能密钥的一半）2.2 对称密码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。古典密码（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，还将数学的方法引入到密码分析和研究中。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（代换技术在现代密码学中也得到了广泛应用。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。一个或多个替换表。替换表就是密钥。Caesar 密码，单表代换密码，多表代换加密））对称密码（流密码（序列密码。古典密码都属于流密码。序列密码的加密和解密每次只处理数据流的一个符号（如一个字符或一个比特）。目前主要应用于军事和外交等机密部门。RC4 流密码算法：种子密钥 K（1~256 个字节）。这个被选出的元素与明文（或密文）异或，实现加密（或解密）。初始化 S：(1)对 S 进行线性填充。(2)用种子密钥填充另一个 256 字节长的 K 表。(3)用 K 产生 S 的初始置换）和分组密码（块密码。如果 $m>n$，则称为带数据压缩的分组密码。如果 $m<n$，则称为带数据扩展的分组密码。绝大部分基于网络的对称密码应用使用的是分组密码））数据加密标准曾经使用最广泛的密码系统。S-P 网络结构，分组长度为 64 位，密钥长度为 56。第一步：变换明文。第二步：按照规则迭代。第三步：逆置换。DES 的安全性——已经不安全。争论的焦点主要集中于密钥的长度和算法本身的安全性。DES 受到的最大攻击是它的密钥长度仅有 56 比特。1998 年 7 月不到三天时间就成功破译了 DES。2000 年 1 月，DES 解密机以 22.5 小时的战绩,成功地破解了 DES 加密算法。DES 的各种变种三重 DES 破解密文需要 2^{112}次穷举搜索。高级加密标准（AES）2001 年 11 月发布了高级加密标准建议所有的分组加密采用 AES。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。公钥密码体制原理传统密码体制是基于替换和置换。公钥算法建立在数学函数基础上。其安全性基于数学上难解的问题。由一个密钥推知另一个密钥，在计算上是不可能的。通信双方无需预先商定密钥就可以进行秘密通信。单向陷门函数。辅助信息（陷门信息）作为私钥基于大整数因子分解问题。基于离散对数问题的。RSA 算法分组密码体制。大整数的素因子分解是困难问题。公开密钥为(e,n)，私有密钥为(d,n)；相比对称密码算法慢几个数量级。2.4 散列函数和消息认证码散列函数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。Hash 函数。H=H(M)。验证该消息的完整性。单向性。强抗碰撞性。弱抗碰撞性。目前（2020 年 10 月）：1 对于安全要求较高的应用，不能使用 MD52 找到 SHA-1 的碰撞是较困难的；SHA-2 是安全的。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。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。消息鉴别码（MAC，密码校验）。基于 Hash 函数导出 MAC 的方法成为了主流。基于 MAC 的鉴别与加密相比，MAC 算法更不易被攻破。CBC-MAC（密文分组链接消息鉴别码）2.5 数字签名签名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。我国的《电子签名法》也规定可靠的数字签名与手写签名或印章有同等法律效力。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。数字签名体制的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。满足：对任意 k∈K，有一个签名算法 Sig 和一个 k 验证算法 Ver_k，使得对任意消息 m∈M，每一签名 a∈A，Ver_k(m,a)=1，当且仅当 a=Sig_k(m)时。数字签名必须具有的 4 个特征可验证性、不可伪造性、不可否认性、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。数字签名和消息鉴别的主要区别数字签名是解决通信双方内部相互攻击的最好方法，它的作用相当于手写签名。用户 A 发送消息给 B，B 只要通过验证附在消息上的 A 的签名，就可以确认消息是否确实来自于 A。同时，因为消息上有 A 的签名，A 在事后也无法抵赖所发送过的消息。消息鉴别通过验证消息完整性和真实性，可以保护信息交换双方不受第三方的攻击，但是它不能处理通信双方内部的相互的攻击，这些攻击可以有多种形式三、身份认证身份认证：确认某个实体是所声称的实体的行为。计算机认证人的身份，称之为用户认证；计算机认证计算机，主要出现在通信过程中的认证握手阶段，称之为认证协议。3.1 用户认证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。基于口令的认证包括静态口令和动态口令。静态口令用户口令是静态的。"用户账户加静态口令"的身份识别方式。所知道的信息。静态口令的认证必须解决两个问题口令存储（明文方式易受字典攻击。口令文件存储的是口令的散列值难于得到口令明文）、口令传输（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单因素。利用系统中存在的漏洞。重放攻击。单向认证。动态口令一次性口令。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，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。动态口令的产生(1)共享一次性口令表。(2)口令序列（单向算法）。(3)挑战—响应方式（随机数）。(4)时间—事件同步机制。电子令牌卡共享同一个用户口令。动态令牌。挑战数据。种子值、随机数值和用户口令。动态口令的技术特点动态性、随机性、一次性、方便性。智能卡 PIN。USBKey 私钥以及数字证书。USBKey 的特点(1)双因子认证（硬件和 PIN 码）。(2)带有安全存储空间。(3)硬件实现加密算法。(4)便于携带、安全可靠。基于 USBKey 的身份认证主要方式(1)基于挑战/应答的双因子认证方式（USBKey 的（硬件）计算单元）(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）基于生物特征的认证以人体具有的唯一的、可靠的、终生稳定的生物特征为依据。难于抵抗指纹克隆技术的攻击！3.2 认证协议)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。单向认证只有一方对另一方进行认证。密钥分配中心（KDC）。会话密钥 K_{AB} 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。在最坏情况下，重放攻击（重播攻击、回放攻击）。对付重放攻击的 2 种方法及其适用场合时间戳（不适合于面向连接的应用）。挑战/应答（不适合于无连接的应用）。3.3Kerbeross 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；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。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。Kerberos 版本 4 密钥分发中心（KDC）以及一个函数库。Kerberos 版本 5 对版本 4 存在的一些缺陷进行了改进：1 加密系统依赖性（DES 已经不安全。用加密类型标记密文可以使用任何加密技术）。2Internet 协议依赖性（允许使用任何类型的网络地址）。3 消息字节顺序（抽象语法表示（ASN.1）和基本编码规则（BER））。4 门票的生命期（版本 4 最大生命期为 1280 分钟。版本 5 任意长度的生命期）5 向前认证。6 域间认证。7 冗余加密。8PCBC 加密。9 会话密钥。3.4PKI 技术 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。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。主要目的就是用来安全、便捷、高效地分发公钥。基于 X.509 证书的 PKI 模型框架,称为 PKIX。PKI 应用系统的组成：1 认证机构(CA)（认证中心）。2 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）3 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）。4 证书作废系统。5 应用接口（API）。X.509 证书包含的信息 1 版本号。2 序列号。3 签名算法标识。4 签发者。5 有效期。6 证书主体名。7 证书主体的公钥信息。8 签发者惟一标识。9 证书主体惟一标识。10 扩展。11 签名。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。PKIX 安全服务和权限管理的相关协议不可抵赖性（数字时间戳 DTS 和数据有效性验证服务器 DVCS）。数据有效性证书。PKI 信任模型信任模型，就是提供用户双方相互信任机制的框架。层次模型、交叉模型、混合模型、桥 CA 模型、信任链模型。四、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。两种授权技术（访问控制技术和 PMI 技术）。资源。客体。"访问"一词可以概括为系统或用户对这些资源的使用。"访问者"通常被称为主体。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。访问控制模型（概念模型）。主体属性用户的级别或种类是主要的主体属性。组别属性。角色属性。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。主体的属性可能还包括其安全状态。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 自主访问控制自主访问控制（DAC）中，由客体的所有者（或控制者）对自己的客体进行管理。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。C2 级。是根据自主访问控制策略建立的一种模型。以用户或用户组的身份。根据来访主体的身份实施访问控制。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。基于主人的访问控制。访问权限关系会被改变。传统 DAC 策略访问权限的管理依赖于所有对客体具有访问权限的主体。自主访问控制主要存在以下三点不足：资源管理比较分散、用户间的关系不能在系统中体现出来，不易管理、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。

HRU、TAM、ATAM 策略 HRU 将访问权限的授予改为半自主式。这种访问权限的授予行为受到安全策略的限制。相当于提案及表决机制，也就是"主体给出提案，管理员裁定是否通过"。TAM 策略和 ATAM 策略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。基于角色/时间特性的 DAC 策略管理角色。正规角色。将角色和自主访问控制结合。增加角色，实现更细粒度的访问控制。基于时间特性的 DAC 策略使得访问权限具有时间特性。主体可以自主地决定其他哪些主体可以在哪个时间访问它所拥有的客体。更细粒度的控制。授权管理集中式管理、分级式管理、所属权管理、协作式管理、分散式管理。访问控制实现技术(1)保护位机制：保护位与客体相关联。Linux 系统的文件访问控制。(2)能力表机制：个客体访问列表（能力表）。能力表与主体相关联。能力表机制提供了一种在运行期间实行访问控制的方式。它在 DBMS 中可能发挥作用。(3)访问控制表（ACLs）机制：访问控制表是目前最流行、使用最多的访问控制实现技术。每个客体有一个访问控制表，是系统中每一个有权访问这个客体的主体的信息。保护位机制就是这样一种简化形式的访问控制表。(4)授权关系表机制：对应访问矩阵中每一个非空元素的实现技术——授权关系表。类似于稀疏矩阵。访问的高效性。自主访问控制的不足之处系统管理员不利于实现统一的全局访问控制。DAC 却存在用户滥用职权的问题。现有大型商用服务器操作系统中的访问控制机制均为等级型自主访问控制。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。自主访问控制的类型自由型、等级型、宿主型。完善自主访问控制机制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。宿主型。拥有者。唯一有权访问该客体访问控制表。4.3 强制访问控制强制访问控制（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。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。安全性标识。数据的标识称为密级。用户的标识称为许可证级别。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。当且仅当用户许可证级别小于或等于数据的密级时，用户才能对该数据进行写操作。防止了敏感数据的泄露。强制访问控制的主要特征权威制定访问规则，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。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。多级安全策略基于系统中主体与客体的分级来决定是否允许访问。安全标签。主体对客体的访问方式向下读、向上读、向下写、向上写。信息的单向流通。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。不足之处集中控制。向上写。无法适应于复杂的现实环境。4.4 基于角色的访问控制 DAC 和 MAC 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，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。以角色为中心的访问控制模型（RBAC）。基本思想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。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 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。简化了授权管理，具有强大的可操作性和可管理性。核心思想是将权限与角色联系起来，通过角色沟通主体和客体。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。角色认证。主体：可以对其他实体实施操作的主动实体。客体：接受其他实体动作的被动实体。用户：试图使用系统的人员。用户标识（UID）。角色：是系统中一组职责和权限的集合。权限：在受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。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。普通的用户、特殊的用户、作废的用户、作审计的用户。角色权限分配：为角色分配一组访问权限。会话：一次会话是用户的一次活跃进程，它代表用户与系统进行交互。活跃角色集（ARS）：会话激活了用户授权角色集的某个子集。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。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。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。授权策略规定何人在何种情况下能访问何种目标。授权策略的基本内容委托策略、SOA（信任源）策略、角色指派策略、动作策略、用户策略、目标访问策略、角色继承策略。RBAC 的优势简化权限管理、灵活表达和实现组织的安全策略、安全性高，有效实现最小权限管理、实用性强。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。4.5 基于属性的访问控制（ABAC）所有权特征。基于属性的访问控制有效解决了具有大规模、强动态性和强隐私性特点细粒度访问控制。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。ABAC 模型四元组(S,O,P,E)。S 表示主体属性，O 表示客体属性，P 表示权限属性，E 表示环境属性。ABAC 系统的两个阶段准备阶段、执行阶段（主要负责对访问请求的响应及对访问策略的更新）ABAC 的不足之处匿名性导致用户可能滥用其所拥有的属性带来的权限。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。ABE 基本概念传统的 ABAC 仅实现了对用户访问过程的控制。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）。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。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。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。平衡更新粒度及计算资源消耗的权限更新机制。4.6PMI 技术 PMI 基础 PMI 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。AA 即属性权威。AC 即属性证书。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。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。PKI 和 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。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，在用户角色与操作权限建立一种映射关系。PMI 技术的授权管理模式 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。PMI 模型对象、权限声称者、权限验证者。PMI 基础设施的结构和应用模型策略实施点（PEPs）、策略决策点（PDP）、属性权威 AA（属性证书的签发者）、属性库（存放属性证书）、策略库。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）。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。属性证书的分发：推模式、拉模式。五、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。隐写术。媒体信息安全。数字信息的安全。版权和使用权。传输和存储中。信息隐藏和加密的主要区别信息加密：通过密钥控制信息的使用权，从而隐藏秘密信息的内容，但没有隐藏秘密信息存在的事实。信息隐藏：掩盖通信过程中存在秘密信息的事实。确保宿主信息中隐藏的秘密信息不被改变或消除，在必要时提供有效的证明信息。信息隐藏技术的分类按载体类型分类、按密钥分类、按嵌入域分类（空（间）域（或时域）和变换域）、按检测是否需要原始载体信息参与分类（非盲检测算法、盲检测算法）、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。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。性能要求是鲁棒性和不可感知性。3 数据隐藏和数据嵌入：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：水印的特定用途）成功的信息隐藏通常需要满足的技术要求 1 透明性或不可感知性：主要指人的感官不可感知。2 鲁棒性：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：抗恶意攻击能力。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：主要指通过技术手段难于判断。5 自恢复性。6 嵌入强度信息量。NEC 算法有较强的鲁棒性、安全性、透明性等。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。空域或像素域算法 LSB 空域算法：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，相当于叠加一个能量微弱的信号，因而在视觉和听觉上很难察觉。算法对信道干扰及数据操作的鲁棒性差。利用像素的统计特征将信息嵌入像素的亮度值中。变换域算法频率域。离散余弦变换（DCT）离散小波变换（DWT）。DCT 变换域算法的基本思想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：按照应用条件选择变换域。预编码或变形。选择某种变换的频域系数序列。隐藏信息量不能很大。抗攻击能力强。数字水印。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。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。NEC 算法鲁棒性、安全性、透明性。隐秘信息应该嵌入原数据中对人感觉最重要的部分。生理模型算法视觉。听觉。JND（临界可察觉差）。5.3 数字水印标记（水印）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。简述各种数字水印的分类与应用。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。综合版权管理系统。可见水印就是嵌入的保护标识是可见的。不可见水印则把水印信息完全隐藏起来。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。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。空域水印第一种是称作"Patchwork"的方法。第二种方法称作纹理块编码。数字图像签名的思想。量化水印算法他们称这种算法为量化索引调制（QIM）。改变图像几何特征的水印算法。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。基于给定灵敏度下的区域敏感性分类。利用了人类视觉系统的亮度掩蔽、边缘掩蔽及纹理掩蔽特性。5.4 数字隐写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。典型数字图像隐写算法 1LSB（最低有效位）隐写算法：非压缩通用数字图像格式。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。隐写算法大都是由 LSB 方法派生出来。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。利用人眼视觉冗余。子块的复杂度，对于复杂度较高的块，人眼的分辨能力较低，因此可以利用这些变化复杂的块来携带秘密信息。PVD 隐藏算法：相邻像素的差异。视觉对复杂变化的图像信号不敏感。4 调色板图像的隐密算法：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。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：视觉上的不可感知性的实现（即视觉的空间屏蔽效应）。6 文本文档信息隐密：对于 html 文件,在注释标签中夹带秘密信息，也是一种可以考虑的方法。确认出版权归属。5.5 数字指纹数字水印是向数字产品中嵌入版权拥有者的一些信息。数字指纹是在原产品中嵌入与用户有关的信息对非法用户进行跟踪。数字指纹是指与用户和某次购买过程有关的信息。数字指纹体制拷贝分发体制、跟踪体制。数字指纹体制也可以分为算法和协议两部分。用户的身份信息及购买过程的描述信息。数字指纹方案的基本要求：保真性、鲁棒性、嵌入量、合谋容忍性、效率。数字指纹编码合谋容忍编码。合谋安全。编码算法。跟踪算法。指纹编码方案的分类确定性跟踪方案和概率性跟踪、连续指纹、离散指纹、随机指纹、特殊的组合结构构造的指纹。主要是概率性跟踪。连续指纹编码方案用户码字中的每一个码元取自一个连续的集合。水印信息。服从正态分布 N(0,1)的随机实数序列 X。CKLS 体制的指纹嵌入方法 DCT 域中幅值最大的前 k 个系数。数字指纹协议非对称指纹体制实现非法用户的不可否认性。匿名数字指纹用户在购买拷贝的过程中不会泄露自己的身份信息。六、主机系统安全技术保证主机数据存储和处理的保密性、完整性、可用性。6.1 操作系统安全技术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。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。TCSEC 是计算机系统安全评价的第一个正式标准。TCSEC6 个规范性的安全要求清晰明确的安全策略、标明其安全级别、严格的鉴别和认证、审计信息必须单独保存专门人员负责、必须能够独立评估、可信机制自身必须受到保护。TCSEC 的 4 个等级、7 个级别 D1 系统最普通的形式是本地操作系统，如 MS-DOS。自主保护类：C1（自主安全保护）。C2（受控存取保护）。强制保护类：B1（标签安全保护）具有 C2 级的所有安全特征，并具有强制访问控制机制。在该级别下，

不允许客体的拥有者改变其存取的许可权限。B2（结构化保护）。B3（安全区域保护）B3 级系统必须设有安全管理员。验证保护：A1（验证设计）。信息技术安全评价准则（ITSEC）。信息技术安全评价的通用准则（CCforITSEC）。等保 2.0。Windows 及 Unix 系统的安全级别：C2 级。ITSECE3 级别等同于 TCSEC 的 C2 级。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 系统的安全机制信任路径功能、信任机制管理。Windows10 安全性概述身份标识和访问控制、信息保护、防恶意软件。及时为系统打上补丁。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。基于安全核构建安全操作系统。引用监视器和安全核把授权机制与能够对程序的运行加以控制的系统环境结合在一起，可以对受控共享提供支持。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。可信计算基（TCB)在 TCSEC 中的定义是：一个计算机系统中的保护机制的全体。TCB 的构成固件和硬件、与安全策略相关的文件、负责安全管理的人员、安全核、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。进程的活动、执行域交换、I/O 操作。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。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，然后围绕它设计操作系统。操作系统安全机制 1 硬件的安全机制（内存保护（确保存储器中的数据能够被合法地访问。访问控制一般可以由硬件来实现）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。写、读、执行访问模式中的最大环号，这三个环号称为环界）I/O 保护）。2 软件的安全机制（标识与鉴别（认证）机制（名称和标识符（ID）。鉴别是对用户身份的真实性进行识别）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））。审计机制。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。Linux 的安全机制 Linux 使用用户名和用户 ID 标识用户，使用口令来鉴别用户。root 违反“完全仲裁”和“最小特权”安全原则。LKM 机制：可加载内核模块。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。能力机制：将 root 拥有的特权分割成一组特权。6.2 数据库安全技术机密性、完整性、可用性。数据库的安全保护需求防止不适当访问、分级保护、防止推断性攻击、数据库的完整性、数据的操作完整性、数据的语义完整性、审计功能。保证数据库管理系统安全的基本方法用户身份认证、存取控制（确保只授权给有资格的用户访问数据库的权限。以多级强制访问控制为核心的系统安全策略）、数据加密、审计追踪与攻击检测。外包数据库安全自己不擅长的东西（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。非完全可信的第三方。充分考虑来自服务提供者本身的恶意操作。外包数据库系统的特定安全机制数据库加密技术（加密解密都应在客户端完成）、密文数据查询策略（直接操作密文数据。同态加密。序列加密。分步查询）、数据库隐私保护（基于推理控制的隐私内容保护、保密信息检索）、数据完整性验证（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。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）、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）。云数据库/云存储安全共同的特征：基于网络的；可以配置、按需分配；虚拟化的存储和数据管理。云存储模式的安全问题身份认证和访问控制、数据存储和传输的保密性、数据隔离、应用安全。云存储安全机制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。密码技术。加固技术）、云存储管控安全机制（主要解决安全管理的问题）、云存储应用安全机制。6.3 可信计算技术 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。可信计算的宗旨是以可信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。其基本思想是建立一个信任根；建立一条信任链。信任的获得方法主要有直接和间接两种方法。七、网络与系统攻击技术利用网络与系统中存在的漏洞和缺陷实施入侵和破坏。7.1 网络攻击概述软件漏洞能被攻击者利用的错误或缺陷。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。29、简述网络攻击的一般流程。(1)系统调查：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：寻找攻击目标系统内部的安全漏洞。步骤(1)和(2)也称为网络探测。(3)实施攻击：实施真正的网络攻击。(4)巩固攻击成果：重点是长期隐蔽潜伏。(5)痕迹清理：消除攻击过程的痕迹。7.2 网络探测也称为网络侦察。尽可能多地了解攻击目标安全相关的各方面信息。网络踩点不要把某位具体人员的直接联系方法或其他不应该暴露的信息填写出来。主动和被动扫描主动式扫描是基于网络的。被动式扫描策略是基于主机的。常见的扫描类型 TCP 连接扫描、TCPSYN 扫描（半连接扫描）、TCPFIN 扫描、TCPACK 扫描、TCPNull 扫描、TCPRPC 扫描、UDP 扫描、ICMP 扫描。7.3 缓冲区溢出攻击缓冲区溢出的基本原理。向目标程序的缓冲区写超出其长度的内容。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。覆盖了邻近的缓冲区，有可能覆盖程序的正确返回地址。分段错误。执行攻击者通过缓冲区溢出植入内存中的特殊指令。对缓冲区溢出攻击的防范(1)缓冲区不可执行，从而阻止攻击者植入攻击代码。(2)编写正确的代码。(3)C 编译器的边界检查。有缓冲区溢出漏洞的进程不能被控制（劫持）7.4 拒绝服务攻击常见的拒绝服务攻击方法的原理利用网络协议的缺陷，采用耗尽目标主机的通信、存储或计算资源的方式来迫使目标主机暂停服务甚至导致系统崩溃。常见的拒绝服务攻击 SYN 泛洪攻击（发送大量伪造的 TCP 连接请求,TCP 连接无法完成第三步握手）、UDP 泛洪攻击、Ping 泛洪攻击、泪滴攻击、Land 攻击、Smurf 攻击常。拒绝服务攻击的防范主机设置、网络设备设置、路由器的设置（使用扩展访问列表、使用 QoS、使用单一地址逆向转发、使用 TCP 拦截、使用基于内容的访问控制）7.5 僵尸网络僵尸网络结构控制者、主机、命令与控制服务器（整个僵尸程序的核心）。僵尸程序的典型结构僵尸主机控制、下载与更新、信息窃取、躲避检测与对抗分析工作机制(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。小端字节序，低字节存放在低地址。将 attack_overflow.c 中 foo 函数的 charbuff[16]改成 charbuff[123]，其他代码不变。通过调试确定 buff 的首地址与返回地址所在栈的距离 Offset。关闭地址随机化、使用 GCC 栈可执行编译选项编译被攻击程序；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（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：（B=$esp（esp 的内容））（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=0x87。(3)ret 语句：查看 esp 的内容，确定被修改的返回地址。八、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。技术层面：防火墙技术、入侵检测技术、“蜜罐”技术、应急响应技术。8.1 防火墙技术防火墙的定义：执行访问控制、根据访问控制规则。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。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。网络防火墙隔离了内部网络和外部网络。防火墙的特性针对所有的通信、只有被授权的通信才能通过防火墙；安全策略、防火墙本身对于渗透攻击必须是免疫的。防火墙采用的常用技术服务控制、方向控制、用户控制、行为控制。防火墙具有的典型功能访问控制功能、内容控制功能、日志功能、集中管理功能、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。防火墙的分类工作原理：网络层防火墙技术和应用层防火墙。防火墙的硬件环境：基于路由器的防火墙和基于主机系统的防火墙。防火墙的功能。包过滤技术工作在网络层。源地址、目的地址、源端口、目的端口、协议类型等。最小特权原则。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。（默认值：丢弃/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。包过滤防火墙的缺点(1)安全性较差。(2)日志功能也十分有限。(3)无法执行某些安全策略。(4)容易受到利用 TCP/IP 规定和协议栈漏洞的攻击。(5)起作用的只是少数几个因素。很少把这种包过滤技术作为单独的解决方案。代理服务技术的缺点：速度较慢、对用户不透明。代理服务技术应用层网关、应用层防火墙。核心是运行于防火墙主机上的代理服务器程序。完全阻隔了网络通信流。代理服务器的实现应用代理服务器（可以在网络应用层提供授权检查及代理服务功能）、回路级代理服务器（一般代理服务器，适用于多个协议）、智能代理服务器、邮件转发服务器。代理服务器防火墙的特点安全性好、能过滤数据内容、可以方便地与其他安全技术合成。代理服务技术的缺点速度较慢、对用户不透明。状态检测技术动态包过滤技术。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。动态的状态信息表。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 TCP 包、UDP 包。状态检测技术的特点和应用结合了包过滤技术和代理服务技术的特点。克服了包过滤技术和代理服务技术的局限性。缺点是状态检测可能造成网络连接的某种迟滞。自适应代理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。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。防火墙的体系结构屏蔽主机防火墙（单宿堡垒主机）、双宿堡垒主机结构。防火墙的应用选用防火墙时要注意防火墙自身的安全性。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。(4)病毒扫描功能。(5)特殊控制需求。防火墙技术的发展智能化、高速度、分布式并行结构、多功能、专业化。8.2 入侵检测技术主动性和实时性。入侵检测的概念若干关键点收集信息并对收集到的信息进行分析。是对入侵行为的发觉。入侵就是试图破坏安全属性的行为。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。识别非法攻击。入侵检测过程信息收集、（关键点）、数据预处理、数据的检测分析、响应。审计记录的两种方法原始审计记录、检测专用的审计记录。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。入侵检测系统（IDS）是完成入侵检测功能的软件、硬件的组合。通用入侵检测模型（CIDF）IDS 体系结构(1)事件生成器。(2)事件分析器。(3)事件数据库。(4)响应单元。(5)目录服务器。入侵检测系统分类 1 基于检测对象的分类：基于主机的入侵检测系统（HIDS，主机系统和本地用户）、基于网络的入侵检测系统（NIDS，分组数据包）、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）。2 基于检测技术的分类：异常检测（基于行为的检测，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）、误用检测（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）3 基于工作方式的分类：离线检测系统（非实时工作）、在线检测系统（实时联机的检测）。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。分布性主要体现在数据收集模块。层次式 DIDS 和协作式 DIDS。入侵检测的研究重点分布式入侵检测、智能入侵检测、高效的模式匹配算法、基于协议分析的入侵检测、与操作系统的结合、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、入侵检测系统自身安全性的研究、入侵检测系统的标准化。Snort 的组成解码器、预处理器（包重组、协议解码、异常检测）、检测引擎、日志/警报子系统、输出插件。8.3“蜜罐”技术主动防御。本质上是一种没有任何产品价值的安全资源。蜜罐技术是一种对攻击方进行欺骗的技术。蜜网又可称为诱捕网络。蜜罐技术的分类按系统功能分类、按系统交互活动级别分类、按服务实现方式分类、按服务提供方式分类。蜜罐技术的核心机制欺骗环境构建机制、威胁数据捕获机制、威胁数据分析机制。蜜罐技术的辅助机制安全风险控制机制、配置与管理机制、反蜜罐技术的对抗机制。蜜罐部署结构蜜网、蜜场。8.4 应急响应技术安全防护技术不能保证系统 100%的安全。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。响应这个词也用处理来代替。CSIRT 的类型内部 CSIRT、国家 CSIRT、协调中心 CC、分析中心 AC、卖方团队、应急响应提供商。应急响应策略全局策略、服务特定策略、基础策略。安全事件的热线响应检查入侵来源、恢复系统正常工作、事故分析、发布安全警报、安全公告、安全建议、咨询、风险评估、安全教育培训、协助其他组织成立自己的 SIRT，建立网络应急与救援队伍。应急响应的主要阶段准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、报告和追踪阶段九、安全审计与责任认定技术 9.1 安全审计所谓审计，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。审计本质上是一种为事后观察、分析提供支持的机制。安全审计则是对系统安全的审核、稽查与计算。安全审计及主要功能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。事后分析及追查取证。安全审计分析用于入侵检测或对安全违规的自动响应。磁盘空间用尽。审计系统的结构集中式结构、分布式结构。分布式系统结构的工作过程主机代理模块、局域网监视器代理。分布式系统结构的优点扩展能力强、容错能力强、兼容性强、适应性强。设计分布式系统时要考虑的主要问题需要处理不同的格式以实现不同节点间互操作、存在保证这些数据完整性和机密性的需求、分析中心设置。审计的数据来源数据采集的完整性和准确性 1 基于主机的数据源：操作系统日志（主要由三个元素来描述，主体、客体和行为。操作系统事件、安全事件和应用程序事件。操作系统日志是首选数据源）、系统日志、应用日志、基于目标的信息（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：网络数据的获取（利用网络适配器的混杂模式）。对受保护系统的性能影响很小或几乎没有。降低了嗅探器本身遭受入侵者攻击的可能性。更容易检测到某些基于网络协议的攻击方法。与受保护主机的操作系统无关。3 其他途径的数据源：设备产生的活动日志、带外数据源。9.2 数字取证应用计算机、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。多态性是指电子证据的表现形式是多种多样的。数字取证的主要步骤收集、检查、分析、报告。主要作用获得证据，打击违法犯罪。其他作用：排除故障、日志监控、数据提取、完善策略、数据恢复。数字取证的分类主机取证和网络取证、事后取证和实时取证、司法取证和非司法取证。数字取证的数据媒介标准的计算机系统、网络设备、外部设备、存储设备、消费电子产品。电子证据的特点和取证基本原则直接目的:得到说明或验证某个事件的证据。电子证据必须满足两个根本属性。可接受性、完整性（真实性、可靠性）。电子证据的特点数字性、技术性、脆弱性（数据的修改可以在瞬间完成）、多态性（电子证据的表现形式是多种多样）、人机交互性（不同计算机操作人员的参与。会对电子证据施加不同的影响）、复合性（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：时效性。(2)取证过程合法性原则：公开进行。(3)多备份原则：至少应制作两个副本。(4)环境安全原则：在安全环境中进行。(5)严格管理过程的原则：共同完成。共同签名。形成完整的证据链。报告不同的解释、不同的听众。9.3 数字取证关键技术和工具标准的文件。特殊数据（删除的文件、松弛空间、空闲区）。收集文件 1 从媒介复制文件：逻辑备份，比特流映像取证工作应该在工作拷贝上进行。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。2 数据文件完整性。3 文件的 MAC 属性。文件的三个时间戳，也称 MACtimes，最后修改时间、最后访问时间、最后状态改变时间。必须妥善保护好时间属性。4 其他技术问题：数据恢复、隐含数据的修复、RAID 阵列数据的收集、关于数据编码和解码。检查数据文件 1 定位文件：工具和技术可以帮助自动完成这个定位过程。2 提取数据：首先必须知道文件的类型。文件类型一般通过扩展名来识别。更精确的方法是查看文件的头部信息。3 使用取证工具进行检测。收集操作系统数据收集易失性数据、收集非易失性数据。十、Internet 安全 10.1OSI 安全体系结构其核心内容是保证异构计算机之间远距离交换信息的安全。安全攻击分成被动攻击（信息收集（内容泄露）、流量分析（判断通信的性质））和主动攻击（伪装（某实体假装成别的实体）、重放（再次发送）、消息修改、拒绝服务）。安全机制用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程，或实现该过程的设备。安全服务一种由系统提供的对系统资源进行特殊保护的处理或通信服务。鉴别服务与保证通信的真实性有关，提供对通信中对等实体和数据来源的鉴别。保证两个实体是可信的。保证该连接不受第三方的干扰。对等实体鉴别。数据源鉴别。访问控制服务包括身份认证和权限验证。数据保密性服务连接保密性、无连接保密性、选择字段保密性、信息流保密性。数据完整性服务带恢复的连接完整性、不带恢复的连接完整性、选择字段的连接完整性、无连接完整性、选择字段无连接完整性。不可否认服务具有源点证明的不可否认、具有交付证明的不可否认。安全机制用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程，或实现该过程的设备。数字签名机制的两个过程签名、验证。访问控制机制访问控制信息库、鉴别信息、能力和属性、安全标号、时间、路径、持续时间。数据完整性机制单个数据单元完整性、数据传输中数据单元序列完整性。鉴别交换机制互换信息确认实体身份。通信业务填充机制对抗通信业务分析。公证机制确证两个或多个实体之间数据通信的特征：数据的完整性、源点、终点及收发时间。5 种辅助的安全机制可信功能、安全标签、事件检测、安全审计跟踪、安全恢复。10.2IPSec 协议 IPSec 将密码技术应用在网络层。IPSec 体系结构 AH 提供数据的完整性、真实性和防重放攻击等安全服务，但不包括机密性。ESP 除了实现 AH 所实现的功能外，还可以实现数据的机密性。安全关联是发送方和接收方之间的受到密码技术保护的单向关系。安全关联的参数安全参数索引(SPI)、目标 IP 地址、安全协议标识（安全关联数据库（SAD）和安全策略数据库（SPD））IPSec 的两种工作模式。(1)传输模式：一般用于在两台主机之间的端到端通信。(2)隧道模式：一般用于两个网络之间的通信。认证头（AH）的结构邻接头、载荷长度、保留、安全参数索引（SPI）、序列号、认证数据（ICV）。ESP 格式安全参数索引（SPI，32 位）、序列号（32 位）、载荷数据（变量）、填充域（0~255 字节）、填充长度（8 位）、邻接头（8 位）、认证数据（变长）。IKE 协议手动、自动。10.3SSL/TLS 协议安全套接层（SSL）协议主要目标是为 Web 通信协议—HTTP 协议提供保密和可靠通信。运行在 TCP 协议栈的传输层。用户级进程。SSL 记录协议的主要步骤应用数据→数据片段→压缩数据→增加 MAC→加密数据和 MAC→增加 SSL 记录头→作为有效载荷片段传递给 TCP。SSL 握手协议的处理过程。建立安全能力->服务器发送证书->客户端发送其证书->结束握手协议。SSL/TLS 协议提供的服务的特性保密性、认证性、完整性。SSL 协议分层模型 1SSL 记录协议。2 三个高层协议：SSL 握手协议、SSL 密码修改协议和 SSL 报警协议。SSL 会话客户端和服务器间的关联。通过握手协议创建。由多个连接共享。会话状态的参数会话标识符、对等实体证书、压缩方法、密码规范、主密码、可恢复性标志。SSL 连接对 SSL 来说，连接表示的是对等网络关系。在一个会话中可以建立多个连接。SSL 记录协议所有的 SSL 通信都使用 SSL 记录层。SSL 修改密码规范协议只包含一个值为 1 的单个字节。10.4 安全电子交易事实上的工业标准。SET 的需求(1)提供支付和订购信息的保密性。(2)确保传送数据的完整性。(3)持卡人账号认证。(4)为商家提供认证。(5)安全技术。(6)创建一个不依赖于传输安全机制也不妨碍其使用的协议。(7)在软件和网络提供者之间提供功能设施和互操作性。SET 的特性(1)信息保密性。(2)数据完整性。(3)持卡人账号认证。(4)商家认证。SET 系统构成持卡人、商家、清算银行、支付网关、认证机构。基于 SET 的交易流程顾客开通账号->顾客申请证书->商家申请证书->顾客进行订购->商家被验证->发送订购和支付信息->商家请求支付认证>商家确认订购->商家提供商品或服务->商家请求付款。双向签名订购信息（OI）。支付信息（PI）。十一、无线网络安全 11.1IEEE802.11 无线网络安全 IEEE802 局域网标准。802.11 无线局域网。物理层和 MAC 层。需要认证技术，以验证节点的身份。无线局域网需要隐私保护机制。数据保密和完整性、身份认证。有线等效隐私（WEP）提供与有线局域网相同级别的安全保护；数据链路层的数据安全。对称流密码体制。开放系统认证是“零认证”。认证过程以明文方式进行（认证请求、认证响应）。以手工的方法将密钥输入到每个设备中。允许最多 4 个密钥存储在每个设备上。WEP 共享密钥认证的主要步骤认证请求→挑战文本→加密的挑战文本→接入成功/失败。WEP 的缺陷静态共享密钥和 IV 重用（当加密的数据包个数超过 224 时，IV 必然发生重复）、认证的漏洞（身份认证是单向的。共享密钥认证也容易导致认证伪造。WEP 协议本身没有抗重放保护机制）。IEEE802.11i 关注无线接入点（AP）和无线工作站点（STA）之间的安全通信。健壮安全网络 RSN（认证、访问控制、带消息完整性的机密性）。IEEE802.11i 强安全网络操作的阶段发现阶段、认证阶段、密钥管理阶段、安全通信阶段、连接终止阶段。TKIP、CCMP 两种数据加密机制，增强了 WLAN 中的数据加密和认证性能。基于 802.1x 的、无线接入点和无线工作站点的双向增强认证机制。IEEE802.11i 支持的安全协议加强的加密算法 CCMP 或 TKIP，其中必须实现基于 AES 的 CCMP。TKIP 将密钥的长度由 40 位增加到 128 位，初始化向量的长度由 24 位增加到 48 位，解决了 WEP 密钥长度太短的问题。TKIP 提高加密强度的新机制每包一密钥、消息完整性校验码（MIC）、具有序列功能的初始化向量（IV）、密钥生成及定期更新功能。TKIP 从如下几个方面加强了 WEP 协议防止消息伪造和其他主动攻击的机制、混合加密函数可以有效地抵抗重放攻击，使密钥更安全、使用 TSC 抵抗重放攻击。TKIP 只是一种过渡算法。CCMP 基于 AES 算法和 CCM 模式，由加密模式和密码块链式消息认证码组成，能解决 WEP 中出现的所有问题。802.1x 认证过程连接到 AS->EAP 交换->安全密钥分发。EAP802.11i 推荐采用 EAP-TLS 方法。EAP-TLS 是一种基于 TLS 的认证方式。密钥管理密钥层次（对等主密钥 PMK、对等临时密钥 PTK、密钥确认密钥 KCK、密钥加密密钥 KEK、临时加密密钥 TEK）。四次握手的目的在于由 STA 和 AP 共享的 PMK 推导单播通信密钥 PTK。11.2 移动通信系统的安全移动互联网的要素无线移动通信网络、公众互联网、移动通信终端。移动通信系统首先必须解决的问题 1 对用户进行认证，防止未注册用户的欺骗性接入；2 对无线路径加密，以防止第三方窃听。移动通信系统还应能提供用户身份保护，防止用户位置泄露。国际移动用户识别码（IMSI）和用户认证密钥（Ki）一起构成了网络籍以鉴别用户的重要“身份证件”。SIM 卡的使用安全相关的运算都在 SIM 卡中进行，以防止密钥的泄露。身份认证问题认证过程是单向的。攻击者利用假的 SGSN 对用户进行欺骗。SIM 卡问题攻击者可以在几分钟内获得 SIM 卡中的密钥信息。从终端用户的角度来说，要防止别人获得自己的终端。其他安全问题 IP 网络的所有安全问题在 GPRS 网络中仍然存在。在利用 GPRS 进行安全通信时，不能只依靠 GPRS 系统本身的安全机制,还应在应用层上加强安全保护。GSM 安全的安全功能？(1)用户身份认证；(2)用户身份保密；(3)用户数据保密以及信令数据保密。3GPP 安全总体结构(1)网络接入安全。(2)网络域安全。(3)用户域安全。(4)应用域安全。(5)安全特性的可视性及可配置能力。十二、恶意代码检测与防范技术 12.1 恶意代码概述广告软件、间谍软件、恶意共享软件、不需要的代码。代码是否独立，可以将其分成独立的和寄生（感染宿主程序）的恶意代码。根据其是否能自我复制（自动传染），可以将其分成广义病毒及普通的恶意代码。传统意义上的病毒是狭义病毒。恶意代码的分类后门（陷阱，秘密入口，绕过正常的访问控制过程）、逻辑炸弹、间谍软件（谍件）、特洛伊木马（木马的功能主要在于削弱系统的安全控制机制，尤其是访问控制机制）、病毒、蠕虫（能完成特定攻击过程的自治软件）、僵尸、P2P 系统、RootKit（RootKit 是一种恶意程序，用于获取目标主机 root 权限之后隐藏攻击者访问痕迹，使得攻击者不被发现，从而能够长期拥有管理员权限）恶意代码长期存在的原因利益驱使、系统和应用软件存在漏洞。12.2 计算机病毒概述狭义病毒，同时具有寄生性和感染性的恶意代码。分类引导型病毒、文件型病毒、混合型病毒、变形病毒、脚本病毒（用脚本语言编写的病毒）、宏病毒（办公自动化程序编制的文档）（脚本病毒和宏病毒保存在文档中）特性感染性（感染性是指病毒具有把自身的拷贝放入其他程序（或文档）的特性）、非授权性、潜伏性（计算机病毒的这种隐蔽自己、使人难以发现的特性称为潜伏性）、可触发性、破坏性（破坏文件或数据，扰乱系统正常工作的特性称为破坏性。极端的恶意攻击，最终目的是获取经济利益）。组成(1)引导模块。(2)感染模块：病毒最核心、最关键的代码。(3)触发模块。(4)破坏模块。12.3 几种常见恶意代码的实现机理 U 盘病毒也称 AutoRun 病毒。12.4 网络蠕虫攻击代码一般分为两个部分：一部分执行感染主机的任务：一部分在被感染的主机上运行。网络蠕虫的组成(1)侦察模块。(2)攻击模块。(3)通信模块。(4)命令接口模块。(5)数据库支持。网络蠕虫的传播利用系统漏洞主动传播、利用电子邮件系统传播、通过局域网传播、通过即时工具传播、多种方式组合传播 12.5 木马反弹端口。木马的最关键特性是隐蔽性。木马的隐藏和伪装绑定到程序中、隐藏在配置文件或注册表中、伪装在普通文件中。12.6 恶意代码检测与分析技术恶意代码检测与分析系统的主要模块技术模块、分析模块。技术模块需要搜集、提取的信息代码的静态结构、表现出有恶意的行为、与操作系统的交互行为。恶意代码动态分析方法系统监控法、动态跟踪法（用户态、内核态、指令模拟器）。恶意代码分类方法相似性、数据挖掘。12.7 恶意代码的防御人是最根本最重要的因素。提高人员的安全防范意识和水平、建立完善的防护系统对系统要经常性的维护和升级、定期对重要的资料进行备份、正确处理受到恶意活动代码攻击的系统。对于个人用户而言安装正版知名的反病毒软件、防火墙和入侵检测系统，并能够正确配置和及时升级。洁身自好，远离不良网站。用虚拟机上网。十三、内容安全技术 13.1 内容安全的概念如果压缩程度不是太高，可以认为它们表达的内容是相同的。内容安全就是指内容的复制、传播和流动得到人们预期的控制和监测。对内容安全的需求数字版权侵权及其控制、不良内容传播及其控制（不良内容的肆意传播是另外一个与内容相关的安全问题）、敏感内容泄露及其控制（敏感信息主要包括保密文件和与知识产权相关的资料等。内容伪造及其控制（人们需要能够核实数字内容的真伪）。主动内容安全技术对被监管的内容先进行预处理，在内容中添加验证信息,在以后的监管中，它通过分析所获得内容中添加的验证信息来判断内容的性质，并实施相应的控制。被动内容安全技术不预先处理被监管的内容，它通过分析获得的内容本身判断内容的性质，并实施相应的控制策略。广义内容安全技术指与内容及其应用特性相关的所有信息安全技术。狭义的内容安全技术主要包括广义内容安全技术中涉及内容搜索、过滤和监控的部分。13.2 文本过滤基于关键字的过滤方法是不良文本过滤早期常用的方法。首先由专业人员编制一个不良文本关键字词库，当匹配超过一定阈值之后，系统就认为这篇文本是不良文本。关键字词有可能在正反两类文本中都频繁出现。敏感字词的滞后性。没有能够准确的联系语境。导致了较高的误判率。基于分级标签过滤方法网络分级目前还是一个自愿采用的分级系统。技术上存在着很大的问题。应根据不同年龄有不同的约束内容。基于地址库过滤方法基于地址库的过滤方法可以分为以下三个类别：IP 地址过滤（通过封锁指定网站的 IP 地址）、URL 过滤（直接定位不良文本在互联网上的具体位置,直接对该网页进行屏蔽）以及 IP 和 URL 相结合的过滤方法（对于一个网站下大部分的网页都是不良信息的情况，则采用 IP 过滤；如果是一个网站下只有极少一部分是不良文本这种情况，则采用 URL 过滤）。基于内容的动态过滤法使用关键字过滤方法有很高的误判率。需要进一步根据文本的具体内容来判断指定文本的具体类别属性。中文分词：将文本中连续的字符串按照一定的算法将其划分为独立的、有实际意义的词。13.3 话题发现和跟踪话题自动发现的流程信息采集阶段（利用网络爬虫工具，从指定的 Internet 网站把 Web 网页等互联网信息资源抓取到计算机本地进行存储）、网络文本处理（也称预处理）、文本内容分词、文本向量化、网络文本聚类、话题热度评估。13.4 内容安全分级监管(1)信息内容分级标准（包括内容分级的词汇表、分级标记和分级操作方法）(2)分级信息的发布（在信息的分级标记，对标记信息自身需要采取保护措施,防止标记信息被篡改）(3)分级信息的使用（信息服务提供层面，信息服务使用层面）13.5 多媒体内容安全技术简介未经授权的访问、复制、发行具有知识产权的数字产品使得数字媒体业遭受了巨大的损失。对数字媒体产品进行有效的权利管理和保护，维护数字多媒体的内容安全,保护数字媒体避免未经授权的访问、复制和发行，成为十分迫切的研究课题。数字多媒体内容安全面临的问题(1)如何鉴别一个数字媒体作品的创建者。(2)如何确定数字媒体作品创建者的版权声明。(3)如何公证一个数字作品的签名与版权声明。(4)如何控制用户访问数字媒体作品的权限。数字权益管理（DRM）技术：提供从数字内容的创作者，到发行者，到消费者的整个价值链的权益保护。

图11-24 3GPP安全体制总体结构