1.绪论

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。习近平指出：**没有网络安全就没有国家安全。**2016 年 12 月 27 日，国家互联网信息办公室发布《国家网络空间安全战略》

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。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】

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】

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】

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。是信息资源服务功能和性能可靠性的度量】

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。包括：信息泄露、非授权的篡改、拒绝服务、非法使用、假冒、抵赖、网络与系统攻击、恶意代码、自然灾害、人为失误和故意破坏】

信息安全威胁种类【信息泄漏（保护的信息被泄露或透露给某个非授权的实体）、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）、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）、非法使用（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）、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）、抵赖（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）、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）、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）、自然灾害、人为失误和故意破坏】

信息安全发展历程【通信安全时期（1949 关注如何保证数据在从一地传送到另一地时的安全性）、计算机安全时期（20 世纪 70～80 年代 以保密性、完整性和可用性为目标的信息安全阶段）、网络安全时期（20 世纪 90 年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）、信息安全保障时代（21 世纪 从整体角度考虑其体系建设的信息安全保障时代）】

信息保障技术框架（IATF）【将信息系统的信息保障技术层面划分成了四个技术框架焦点域：网络和基础设施、区域边界、计算环境和支撑性基础设施。其核心思想是纵深层防御战略，采用多层次、纵深的安全措施来保障用户信息及信息系统的安全，人、技术和操作是三个主要核心要素。其他安全原则：保护多个位置、分层防御、安全健壮性】

2.密码技术

一般意义上的密码≠密钥，密码是一串字符，密钥是加密/解密过程中的参数。

两种密码体制【对称密码（加密解密使用相同的密钥，分为流密码和分组密码）和非对称密码（加密解密使用不同的密钥，公钥用于加密，私钥用于解密）】

密码在计算上安全【破译密码的代价超出密文信息的价值、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、穷举攻击】

密码分析攻击【唯密文攻击（仅已知密文）、已知明文攻击（已知一些密文信息及其对应的明文或某段明文信息的格式）、选择明文攻击（选择某些认为对攻击有利的明文，并获取其相应的密文）、选择密文攻击（已知一些密文，并通过加密算法解密，获得解密后的明文）】

古典密码【以字符为基本加密单元，体现了现代密码学的两大基本思想：置换（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）和代换（将明文字母替换成替他字母、数字或符号，替换表就是密钥）】

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】

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。常见的分组算法有 DES、DES3、IDEA、AES 等】

公钥密码体制【公钥密码体制则将加密密钥、解密密钥甚至加密算法、解密算法分开，用户只需掌握解密密钥，而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实际应用中，公钥密钥和对称密码经常结合起来使用，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【1.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。2.由一个密钥推知另一个密钥，在计算上是不可能的。3.通信双方无需预先商定密钥就可以进行秘密通信】

数据加密标准 DES【对称密码、分组密码体制，分组长度为 64 位，密钥长度为 56】**高级加密标准 AES**【对称密码、分组密码体制】**RSA**【非对称密码体制，其理论基础是“大整数的素因子分解是困难问题”的结论】

RC4【对称密码、流密码体制】

散列函数【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】

散列函数的安全性【单向性、强抗碰撞性、弱抗碰撞性】

MD5 散列函数【散列码长度为 128bit】**SHA 序列函数**【SHA-1 散列码长度为 160bit，SHA-2 散列码长度为 256、384 和 512 位】

消息鉴别【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】

数字签名【起到了鉴别、核准、负责等作用，其基本目的是认证、核准和负责，防止相互欺骗和抵赖。具有可验证性、不可伪造性、不可否认性、数据完整性的特征。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】

数字签名的特征【可验证性、不可伪造性、不可否认性、数据完整性】

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，也叫基本密钥或初始密钥；2.会话密钥；3.密钥加密密钥；4.主机主密钥】

3.身份认证

身份认证【确认某个实体是所声称的实体的行为。用户认证（计算机认证人的身份，是对访问者授权的前提），认证协议（计算机认证计算机）】

用户认证【基于口令的认证（静态口令，动态口令）、基于智能卡的认证（USB Key 存储用户的私钥以及数字证书）、基于生物特征的认证（唯一的、可靠的、终生稳定的）】

静态口令【口令存储（一般系统的口令文件存储的是口令的散列值，即使攻击者得到口令文件，由于散列函数的单向性，也难以得到口令明文）、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】

动态口令【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。主要思路是在登录过程中加入不确定因素，产生一个无法预测的动态口令。动态口令具有以下几个技术特点：动态性、随机性、一次性、方便性】

动态口令的产生【共享一次性口令表、口令序列、挑战-响应方式、时间-事件同步机制】

USB Key【可以存储用户的私钥以及数字证书。具有以下 4 个主要特点：双因子认证、带有安全存储空间、硬件实现加密算法、便于携带，安全可靠】

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、相结合的计算机文件】

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），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）】

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。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。主要目的是用来安全、便捷、高效地分发公钥】

PKI 应用系统的组成【认证机构 CA（是数字证书生成、发放的运行实体，在其上常常运行着一个或多个注册机构）、数字证书库（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（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来完成）、应用接口 API】

PKIX【基于 X.509 证书的 PKI 模型框架】

X.509 证书【版本号、序列号、签名算法标识、签发者、有效期、证书主体名、证书主体的公钥信息、签发者唯一标识、证书主体唯一标识、扩展、签名】

CA 用它的私钥对证书签名，如果用户知道相应的公钥，则用户可以验证 CA 签名证书的合法性

CA 的主要职能【1.制定并发布本地 CA 策略；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】

PKI 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】

4.授权与控制访问技术

授权【给已通过认证的用户授予相应的权限。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。授权技术：访问控制技术和 PMI 技术】

主体与客体【系统或用户对这些资源的使用，访问者通常被称为主体。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。】

主体属性【级别、种类、相关执行程序的性质、所处的网络或物理地址、安全状态】

客体属性【所允许的操作及其信息级别、安全状态】

自主访问控制 DAC【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。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。客体的主人全权管理有关该客体的访问授权】

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。缺点：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 策略【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”】

基于角色/时间特性的 DAC 策略【增加角色，实现更细粒度的访问控制。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，实现了更细粒度的控制】

自主访问控制的授权管理（Linux、UNIX、Windows Server）【集中式、分级式、所属权、协作式、分散式】

实现技术【保护位机制、能力表机制（能力表机制提供了一种在运行期间实行访问控制的方式）、访问控制表机制（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）、授权关系表机制】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

自主访问控制的缺点【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；在许多组织中，用户对他们所能访问的资源并不具有所有权，组织本身才是系统中资源的真正拥有者。而且，各组织希望访问控制与组织内部的安全策略相一致，并由管理部门统一实施访问控制，不允许用户自主地处理，而 DAC 却存在用户滥用职权的问题；用户间的关系不能在系统中体现出来，不易管理；信息容易泄露，不能抵御特洛伊木马的攻击】

强制访问控制 MAC（SELinux、多级安全 MLS）【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。基于系统权威制定的访问规则来对访问进行控制】

强制访问控制基本概念【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。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，该用户才能对该数据进行写操作】

强制访问控制主要特征【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】

强制访问控制的优缺点【优点是安全性较高，对特洛伊木马攻击有一定的抵御作用，即使某用户进程被特洛伊木马非法控制，也不能随意扩散机密信息。缺点是完整性方面控制不够；应用领域比较窄。由于强制访问控制的规则制定严格并且缺乏弹性，无法适应于复杂的现实环境】

基于角色的访问控制 RBAC（在线系统）【基本思想为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。核心思想是将权限与角色联系起来。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。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】

RBAC 的优点【简化权限管理；灵活表达和实现组织的安全策略；安全性高，该策略可以有效实现最小权限管理；实用性强】

5.信息隐藏技术

信息隐藏【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。现代信息隐藏是一种解决媒体信息安全的新方法，通过把秘密信息永久地隐藏在可公开的媒体信息里，达到证实该媒体信息的所有权归属、验证数据完整性或传递秘密信息的目的，从而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】

信息加密与信息隐藏的区别【信息加密利用密钥把信息变换成密文，通过公开信道传输。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的事实。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【按载体类型分类（有文本、图像、音频和视频的信息隐藏技术）、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）、按嵌入域分类（可分为空(间)域(或时域)和变换域方法）、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）、按照保护对象分类（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；数字水印：它是指嵌在数字产品中的数字信号。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；数据隐藏和数据嵌入：一般指隐写术，或者指介于隐写术和水印之间的应用；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

信息隐藏的技术要求【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。主要指人的感官不可感知）、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）、安全性（具有较强的抗恶意攻击能力，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）、不可检测性（指通过技术手段难于判断）、自恢复性、嵌入强度（隐藏的信息越多，鲁棒性就越差）】

隐藏信息的基本算法【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【1.(LSB)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；2.(Patchwork)利用像素的统计特征将信息嵌入像素的亮度值中。缺陷是嵌入的信息量较低，大信息量嵌入就需要牺牲其鲁棒性】

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(DCT)和离散小波变换(DWT)。DCT 是静态数字图像压缩编码标准 JPEG 和运动图像压缩编码标准 MPEG2.0 的核心算法。DWT 是静态数字图像压缩编码标准 JPEG-2000 和运动图像压缩编码标准 MPEG-4 的核心算法。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【按照应用条件选择变换域；根据待隐藏的隐秘信息的类型，对它进行适当的预编码或变形，以提高嵌入的信息量；根据隐藏信息量的大小和其相应的安全目标，有目的地选择某种变换的频域系数序列】

数字水印【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。主要包括水印嵌入与水印提取两个环节】

数字水印的分类与应用【鲁棒性水印（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）和脆弱性水印（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）、可见水印（嵌入的保护标识是可见的，台标）和不可见水印（把水印信息完全隐藏起来，为了获得惩罚盗版者的证据）、私有水印（检测水印时必须采用原始数据作为参照）和公有水印（不需要采用原始数据进行检测）、对称水印（嵌入与提取互逆）和非对称水印（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）、多比特水印和 1 比特水印（如果嵌入的水印信号没有具体含义，只是表示“有水印”或“无水印”两种情况，称为 1 比特水印。而嵌入多比特有意义的信息（如版权所有者姓名、地址、出品时间）的水印称为多比特水印）】

空域水印【“Patchwork”的方法、纹理块编码】

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】

现代隐写技术的模型【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】

数字图像隐写算法【LSB（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）；自适应嵌入：基于位平面复杂度分割的隐写算法 BPCS（利用人眼视觉冗余的信息隐藏方法。具体做法是，将图像的多个位平面分块，计算所分子块的复杂度，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（根据相邻像素的差异情况来确定图像的复杂程度）；JPEG 图像隐写算法；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）；二值图像的信息隐密；文本文档信息隐密】

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。为了提高隐藏容量，很多隐写方法利用人类视觉特性进行自适应嵌入，把最低有效位方法进行了推广，不但利用图像最低位平面来携带信息，其他符合条件的位平面也参与携带信息】

数字水印与数字指纹【数字水印是向数字产品中嵌入版权拥有者的一些信息，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。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】

数字指纹【在原产品中嵌入与用户有关的信息，产品提供者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。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【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。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【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，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。现有的指纹编码方案主要是概率性跟踪方案】

数字指纹协议【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。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】

6.主机系统安全技术

主机系统安全【保证主机数据存储和处理的保密性、完整性、可用性。操作系统安全是主机系统安全的核心】

可信计算机评价标准 TCSEC【是计算机系统安全评价的第一个正式标准。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【D 类（D1 最低 Windows95，98）、C 类自主保护类（C1 自主安全保护，C2 受控存取保护 Windows，Linux）、B 类强制保护类（B1 标签安全保护，B2 结构化保护，B3 安全区域保护）、A 类验证保护（A1 验证设计）】

达到 C2 安全级的 4 项关键要求【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 10 安全性【Windows 10 执行的安全性工作有三大类：1.身份标识和访问控制；2.信息保护；3.防恶意软件】

安全核【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。定义：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。基于安全核构建安全操作系统具有两个方面的优势：1.减轻应用系统的负担，避免出现安全隐患；2.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】

可信计算基 TCB【TCB 在 TCSEC 中的定义：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】

安全核与 TCB【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】

安全操作系统的设计方法【分离法（Android 系统）、安全核法（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）、仿真法】

硬件系统安全机制【内存保护（确保存储器中的数据能够被合法地访问）、运行域保护（运行域是进程运行的区域，可以看成是一系列的同心圆，最内层硬件的特权最高，最外层用户的特权最低）、I/O 保护】

软件系统安全机制【标识与鉴别机制（用名称和标识符(ID)来标明系统中的一个用户，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）】

Linux 的安全机制【标识与鉴别机制（Linux 使用用户名和用户 ID 标识用户，使用口令来鉴别用户）、安全注意键（按下后，保证用户看到真正的登录提示，而非登录模拟器，即保证是真正的登录程序读取用户的账号名和口令）、LKM 机制（可加载内核模块，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）、能力机制（该机制将 root 拥有的特权分割成一组特权）、日志系统、防火墙机制】

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】

保证数据库安全的基本方法【用户身份认证、存取控制、数据加密、审计追踪与攻击检测】

外包数据库系统的安全机制【包含一般机制的同时，还有数据库加密技术（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）、密文数据查询策略、数据库隐私保护、数据完整性验证（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）、外包数据库版权保护】

云存储【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【身份认证和访问控制问题、数据存储和传输的保密性问题、数据隔离问题、应用安全问题】

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，密码技术和加固技术）、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】

可信计算组织 TCG【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【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】

可信计算的基本思想【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：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。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】

信任的获得方法主要有直接和间接两种方法

7.网络与系统攻击技术

网络与系统攻击【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、入侵和破坏】

网络攻击一般流程【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）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）】

网络探测&网络侦查【1.网络踩点；2.网络扫描（主动&被动）和查点】

常见的扫描类型【TCP 连接扫描、TCP SYN 扫描（半连接扫描）、TCP FIN 扫描、TCP ACK 扫描、TCP Null 扫描、TCP RPC 扫描、UDP 扫描、ICMP 扫描】

缓冲区溢出攻击【基本原理是攻击者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，以达到攻击的目的。原因是程序中没有仔细检查用户输入的参数】

缓冲区溢出的防范【1.使接收转入数据的缓冲区不可执行；2.编写正确的代码；3.边界检查】

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】

僵尸网络【是攻击者出于恶意目的，融合传统的恶意软件，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】

僵尸网络的结构【控制者（命令的发起者，即控制僵尸网络的攻击者。控制者通过控制程序给僵尸网络发布攻击命令、更新僵尸程序、设置攻击类型等）；主机（俗称“肉鸡”，是一个被僵尸程序感染的主机。僵尸程序秘密运行在被感染的主机中，可以接收控制者发布的命令并执行命令）；命令与控制服务器（控制者与僵尸主机通信的平台。控制者通过命令与控制服务器发布命令，僵尸主机则通过命令与控制服务器接收命令并向控制者发送命令执行报告。）】

僵尸程序的结构【命令与控制模块、传播模块、信息窃取模块、僵尸主机控制模块、下载与更新模块、躲避检测与对抗分析模块】

僵尸网络的工作机制【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】

8.网络与系统安全防护

安全防护【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。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】

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。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。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】

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）；2.只有被授权的通信才能通过防火墙；3.防火墙本身对于渗透攻击必须是免疫的】

防火墙的常用技术【服务控制、方向控制、用户控制、行为控制】

防火墙的功能【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【不能防御不经由防火墙的攻击；不能防范来自内部的威胁；不能防止病毒感染的程序和文件进出内部网；不能防止数据驱动式的攻击】

包过滤技术【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。具体实现为 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】

代理服务技术【核心是运行于防火墙主机上的代理服务器程序。代理服务器防火墙完全阻隔了网络通信流】

状态检测技术【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。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】

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】

入侵检测【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。】

入侵检测的过程【1.信息收集（从网络或系统的关键点得到原始数据）；2.数据预处理（将数据转化为检测器所需要的格式，也包括对冗余信息的去除）；3.数据的检测分析（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）；4.响应（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【原始审计记录&检测专用的审计记录。每个审计记录包含：主体（行为的发起者）、动作（主体对一个对象的操作或联合一个对象完成的操作）、客体（行为的接收者）、异常条件、资源使用、时间戳】

入侵检测系统【事件生成器（采集和过滤事件数据的程序或模块）、事件分析器（分析事件数据和任何 CIDF 组件传送给它的各种数据）、事件数据库（存放各种原始数据或已加工过的数据）、响应单元（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）、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【监测并分析用户和系统的活动、核查系统配置与漏洞、识别已知的攻击行为并报警、统计并分析异常行为、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】

入侵检测系统分类【基于检测对象的分类（基于主机的入侵检测系统、基于网络的入侵检测系统、混合式入侵检测系统）；基于检测技术的分类（异常检测、误用检测）；基于工作方式的分类（离线检测系统、在线检测系统）】

异常检测【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【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】

分布式入侵检测【采用多个代理在网络各部分分别进行入侵检测，各检测单元协作完成检测任务，并还能在更高层次上进行结构扩展，以适应网络规模的扩大。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】

分布式入侵检测的分类【层次式 DIDS（定义了若干个分等级的监测区域，每一个区域有一个专门负责分析数据的 IDS，每一级 IDS 只负责所监测区域的数据分析，然后将结果传送给上一级 IDS）和协作式 DIDS（将中央检测服务器的任务分配给若干个互相合作的基于主机的 IDS，这些 IDS 不分等级，各司其职，负责监控本地主机的某些活动，所有的 IDS 并发执行并相互协作）】

分布式入侵检测系统结构【主机代理模块（审计收集模块作为后台进程运行在监测系统上。它的作用是收集有关主机安全事件的数据，并将这些数据传至中心管理员）、局域网监视代理模块（其运作方式与主机代理模块相同。但它还分析局域网的流量，将结果报告给中心管理员）、中心管理员模块（接收局域网监视模块和主机代理模块送来的报告，分析报告，并对其进行综合处理以判断是否存在入侵）】

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】

蜜罐【主动防御技术，对攻击方进行欺骗的技术，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】

蜜网【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。与蜜罐不同的是，蜜网融入了数据捕获、数据分析和数据控制等元素】

蜜罐的核心机制【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】

应急响应【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】

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、报告与追踪阶段】

9.安全审计与责任认定技术

安全审计【审计就是记录和分析用户使用信息系统过程中的相关事件。安全审计则是对系统安全的审核、稽查与计算】

安全审计的功能概述【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。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】

安全审计的主要功能【安全审计自动响应（指当审计系统检测出一个安全违规事件（或者是潜在的安全攻击）时做出的响应）、安全审计数据生成（规定了对与安全相关的事件进行记录，包括鉴别审计层次、列举可被审计的事件类型，以及鉴别由各种审计记录类型提供的相关审计信息的最小集合）、安全审计分析（定义了分析系统活动和审计数据，来寻找可能的或真正的安全违规操作，可以用于入侵检测或对安全违规的自动响应）、安全审计浏览（主要是指经过授权的管理人员对于审计记录的访问和浏览）、安全审计事件存储（主要是指对审计记录的维护，如何保护审计、如何保证审计记录的有效性，以及如何防止审计数据的丢失）、安全审计事件选择（指管理员可以选择接受审计的事件）】

审计系统的结构【集中式结构、分布式结构（扩展能力强、容错能力强、兼容性强、适应性强）】

审计的数据来源【基于主机的数据源（操作系统日志、系统日志、应用日志、基于目标的信息）、基于网络的数据源、其他途径的数据源】

数字取证【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。概括为以下几点：1.获得证据，打击违法犯罪；2.排除故障；3.日志监控；4.数据恢复；5.数据提取；6.完善策略】

数字取证的分类【主机取证与网络取证、事后取证与实时取证、司法取证与非司法取证】

数字取证的数据媒介【标准的计算机系统、网络设备、网络设备、外部设备、消费电子产品】

电子证据的根本属性【可接受性、完整性（真实可靠）】

电子证据的特点【数字性（计算机证据的物质载体是电子元器件和磁性材料等）、技术性（计算机证据的产生、储存和传输及其采集、分析和判断都必须借助于计算机科学中的计算技术、存储技术、网络通信技术等）、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）、复合性（电子证据是多种形式证据的集合）】

数字取证原则【及时性原则、取证过程合法性原则、多备份原则、环境安全原则、严格管理过程原则】

数字取证过程【收集（发现潜在的数据源并从中获取数据）、检查（评估数据与特定事件的关联性，从收集的数据中提取信息）、分析（分析提取的数据进而依据系统的方法得出结论）、报告】

10.Internet 安全

OSI 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【任何危及企业信息系统安全的活动。网络攻击是指降级、瓦解、拒绝、摧毁计算机或计算机网络中的信息资源，或者降级、瓦解、拒绝、摧毁计算机或计算机网络本身的行为】

被动攻击【试图收集、利用系统的信息，但不影响系统的正常访问，数据的合法用户对这种活动一般不会觉察到。具体分为：信息收集（造成传输信息的内容泄露）、流量分析（可以判断通信的性质）】

主动攻击【是攻击者访问他所需信息的故意行为，一般会改变系统资源或影响系统运作。具体分为：伪装（某实体假装成别的实体）、重放（将攻击者获得的信息再次发送，从而导致非授权效应）、消息修改（攻击者修改合法消息的部分或全部，或者延迟消息的传输以获得非授权作用）、拒绝服务（攻击者设法让目标系统停止提供服务或资源访问，从而阻止授权实体对系统的正常使用或管理）】

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。具体分为：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）、访问控制（服务包括身份认证和权限验证，用于防止未授权用户非法使用或越权使用系统资源）、数据保密性服务（防止网络各系统之间交换的数据被截获或被非法存取而泄露。分为：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（信息流保密性、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（用于防止发送方在发送数据后否认发送，以及接收方在收到数据后否认收到或伪造数据的行为。分为：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。具体分为：加密机制（提供对数据或信息流的保密，并可作为其他安全机制的补充）、数字签名机制（允许数据单元的接收方确认数据单元来源和数据单元的完整性，并保护数据，防止被人伪造）、访问控制机制、数据完整性机制（一是单个数据单元或字段的完整性；二是数据单元或字段序列的完整性）、鉴别交换机制（通过互换信息的方式来确认实体身份的机制）、通信业务填充机制（能用来提供各种不同级别的保护对抗通信业务分析）、路由选择机制（提供动态路由选择或预置路由选择）、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）】

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】

IPSec【将密码技术应用在网络层，提供端对端通信数据的私有性、完整性、真实性和防重放攻击等安全服务。IPSec 通过多种手段提供 IP 层安全服务】

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。一个安全关联由三个参数唯一确定（安全参数索引、目标 IP 地址、安全协议标识）】

IPSec 的 2 种工作模式【传输模式（主要为直接运行在 IP 层之上的协议，如 TCP、UDP 和 ICMP，提供安全保护，一般用于在两台主机之间的端到端通信）、隧道模式（对整个 IP 包提供保护。为了达到这个目的，当 IP 数据包附加了 AH 或 ESP 域之后，整个数据包加安全域被当做一个新 IP 包的载荷，并拥有一个新的外部 IP 头。一般用于两个网络之间的通信）】

AH 协议【IP 认证头(AH)协议为 IP 数据包提供数据完整性校验和身份认证，还有可选择的抗重放攻击保护，但不提供数据加密服务。认证基于消息鉴别码(MAC)，双方必须共享同一个密钥】

ESP 协议【封装安全载荷(ESP)协议为 IP 数据包提供数据完整性校验、身份认证和数据加密，还有可选择的抗重放攻击保护。ESP 用一个密码算法提供机密性，数据完整性则由身份验证算法提供。通过插入一个唯一的、单向递增的序列号提供抗重放服务。只有选择了身份认证时，才可以选择抗重放服务】

安全套接层 SSL【主要目标是为 Web 通信协议—HTTP 协议提供保密和可靠通信。SSL/TLS 被设计为运行在 TCP 协议栈的传输层之上，使得该协议可以被部署在用户级进程中，而不需要对操作系统进行修改。】

SSL 的特性【保密性、认证性、完整性】

SSL 会话【是一个客户端和服务器间的关联，会话是通过握手协议创建的，定义了一组密码安全参数，这些密码安全参数可以由多个连接共享。一个会话状态由以下参数定义：会话标识符、对等实体正式、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【整个操作过程为应用数据分解为数据片段、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【允许客户端和服务器彼此认证对方，并且在应用协议发出或收到第一个数据之前协商加密算法和加密密钥。阶段 1：建立安全能力，包括协议版本、会话标识、密码组、压缩方法和初始随机数；阶段 2：服务器发送证书，交换密钥，证书请求，hello 完成消息；阶段 3：如果接收到请求，客户端发送其证书，发送交换密钥，也可以发送证书验证消息；阶段 4：改变密码组，结束握手协议】

安全电子交易协议 SET【用于保护基于信用卡在线支付的电子商务的安全协议】

SET 的需求【提供支付和订购信息的保密性、确保传送数据的完整性、持卡人账号认证、为商家提供认证、安全技术、创建一个不依赖于传输安全机制也不妨碍其使用的协议、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【信息保密性、数据完整性、持卡人账号认证、商家认证】

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】

L1.无线网络安全

有线等效隐私 WEP【以为无线局域网提供与有线局域网相同级别的安全保护为目的，用于保护无线局域网中的数据链路层的数据安全。WEP 包含以下三个要素：共享密钥 K、初始向量和 RC4 流密码算法。】

/WEP 认证【开放系统认证（本质上是一种空认证机制，认证过程以明文方式进行）、共享密钥认证（1.客户端向接入点发送身份验证请求。2.接入点会回复明文质询。3.客户端使用配置的 WEP 密钥对质询文本进行加密，然后在另一个身份验证请求中将其发送回。4.接入点解密响应。如果这与质询文本匹配，则接入点将发送肯定答复。）】

/WEP 密钥【IEEE 802.11b 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】

802.11i 安全标准【关注无线接入点和无线工作站点之间的安全通信，引入了健壮安全网络 RSN 的概念，定义了以下安全服务：认证（定义用户和网络的交互，以提供相互认证，并生成用于 STA 和 AP 之间无线通信的短期密钥）、访问控制（对认证功能的增强，能与多种认证协议协同工作，带消息完整性的机密性（MAC 层数据与消息完整性校验码一起加密以提供机密性和完整性）。802.11i 中的认证、授权和接入控制主要是由三个部分配合完成的，分别是 802.1x 标准、EAP 协议和 RADIUS 协议】

802.11i 操作【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】

GSM 安全机制（2G）【每个 GSM 用户用国际移动用户识别码 IMSI 唯一标识，并由网络统一分配用户认证密钥 Ki。IMSI 和 Ki 一起构成了网络籍以鉴别用户的重要“身份证件”】

GSM 的安全机制【用户身份认证、用户身份保密、用户数据保密以及信令数据保密】

通用分组无线业务 GPRS（2.5G）【通过增加一些网络节点给移动用户提供无线分组接入服务，提供端到端的、广域的无线 IP 连接】

3G 系统的安全体系【3GPP(WCDMA) 和 3GPP2(cdma2000)】

L2.恶意代码攻击

恶意代码【是任何的程序或可执行代码，其目的是在用户未授权的情况下更改或控制计算机及网络系统。是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行、侵犯用户合法权益的软件。是指故意编制或设置的、对网络或系统会产生威胁(或潜在威胁)的计算机代码】

恶意代码的分类【根据其代码是否独立，可以将其分成独立 (不需要寄宿) 的和寄生的恶意代码；根据其是否能自我复制(自动传染)， 可以将其分成 “无病毒及普通的恶意代码”，传统意义上的病毒是狭义病毒，指同时具有寄生和传染能力的恶意代码】

恶意代码攻击流程【寻找目标、将自身保存在目标之中、触发目标系统中均恶意代码执行，让自身长期存活于目标系统中】

恶意代码攻击技术【代码注入技术、缓冲区溢出攻击技术、三线程技术、端口复用技术、端口反向链接技术】

恶意代码生存技术【反跟踪技术、加密，加壳技术、变形技术】

病毒的分类【引导性病毒、文件型病毒、混合型病毒、变形病毒、脚本病毒、宏病毒】

病毒的特性【感染性（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、可触发性、破坏性（破坏文件或数据， 扰乱系统正常工作）】

病毒的结构【引导模块（病毒的入口模块，它最先获得系统的控制权。引导模块首先将病毒代码引导到内存中的适当位置，其次调用感染模块进行感染，然后根据触发模块的返回值决定是调用病毒的破坏模块还是执行正常的程序）、感染模块（负责完成病毒的感染功能， 这是病毒最核心、最关键的代码。它寻找要感染的目标文件，判断该文件是否已经被感染？。如果没有被感染，则进行感染，并标上感染标志）、触发模块（对预先设定均条件进行判断，如果满足则返回真值，否则返回假值）、破坏模块（完成具体的破坏作用）】

网络蠕虫【是一种自治的、 智能的恶意代码（ 广义上的病毒），可以看作是自动化的攻击代理。蠕虫不需要附在别的程序内，可能不用使用者介入操作也能自我复制或执行】

蠕虫的结构【依察模块（系统向可能的攻击目标发送扫描数据报，探测有用信息。根据返回的信息，该模块就可以判断目标主机当前是否处于活动状态，哪些端口是开放的，以及正在运行的操作系统相关信息等，进一步也还可以搜集到机器的重要配置情况）、攻击模块（通过该模块可在非授权青形下侵入系统、获取系统信息，必要时可在被入侵系统上提升自己的权限）、通信模块（用于实现与蠕虫制作者及其它蠕虫之间的信息交互），命令接口模块、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】

恶意代码检测与分析系统的主要模块【技术模块（主要作用是从恶意代码中搜集、提取有用数据（比如特征码）供分析模块分析使用，这里通常会使用到统计、分析和数据挖掘等技术）；分析模块（用于分析从技术模块获取的数据，根据这些数据建模，比较来判断一个程序是否符合某个或者某类恶意代码的特征，从而判断该程序是否为恶意代码）】

攻术模块需要搜集的信息【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】

恶意代码静态分析方法【指不实际运行恶意程序，只是通过反汇编、反编译等技术来查看代码进行分析。包括：基于特征码检测、基于代码语义检测、启发式扫描方法】

恶意代码动态分析方法【指在代码运行时，通过监视程序的行为、比较运行环境的变化来进行检测与分析。包括：系统监控法、动态跟踪法（基于程序态的行为监测技术、基于内核态的行为监测技术、基于指令模拟器的行为监测技术）】

恶意代码分类方法【基于相似性计算的分类方法、基于数据挖掘的分类方法】

恶意代码的防御【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】

L3.内容安全技术

内容安全【指内容的复制、传播和流动得到人们预期的控制和监测。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】

内容安全的需求【数字版权侵权及其控制（对数字版权的侵权仅仅依靠非法术手段是不够的，数字内容制作企业、内容制作者及管理部门也迫切需要有遏制版权侵权的技术手段），不良内容传播及其控制，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（需要能够核实数字内容的真伪）】

不良文本过滤主要方法【基于关键字的过滤方法（首先由专业人员编制一个不良文本关键字词库，当有文本到来之后，对文本全文进行检索，通过比较简单的布尔逻辑运算进行匹配，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，给予过滤）、基于分级标签过滤方法（通过对不同网页的限相内容赋予不同的级别，以实现过滤）、基于地址库过滤方法（IP 过滤是指通过封锁指定网站的 IP 地址、URL 过滤方法直接定位不良文本生互联网上的具体位置，直接对该网页进行屏蔽。对于一个网站下大部分均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（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）】

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（把互联网网页源码信息进行处理，包含删除无关字符清洗源码、 提取正文和必要的附带信息），文本内容分词（是在汉语文本处理，且选择词语作为文档特征表达的特定情况下必要的一个步骤），文本向量化（汇总分词后文本中的词语，将这些词语作为空间向量的维度构建文本表示的多维向量，然后将各词的文档词频统计值和逆文档词频统计值运用 TFIDF 公式转换为一个权重值，用以表示文本在这个词语代表的维度上的值，进而将文本表示为一组关键词及其词频为权重的空间向量），网络文本聚类（采取一定的组织策略调度文本向量参与相似度计算，并建立话题的向量表示方法），话题热度评估（综合考虑话题中所有报道的点击数、回帖数、报道频率和时间频率等参数，来评估该话题受到关注的程度）】

数字多媒体内容安全的问题【如何鉴别一个数字媒体作品的创建者、如何确定数字媒体作品创建者的版权声明、 如何公证一个数字作品的签名与版权声明、如何控制用户访问数字媒体作品的权限】

2020 试题

1.习近平指出：没有**网络安全**就没有国家安全。网络安全指的是网络与信息系统的信息安全。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。

2.信息安全的目标是保护网络与信息系统中信息的不可抵赖性和可控性等**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。

3.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。

4.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。

5.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。DES 属于**对称密码**体制，AES 属于对称密码体制，RSA 属于**非对称密码**体制。

6.在大规模的互联网应用中交换密钥，应该选用**非对称密码**体制；为了验证信息确实来自某个实体，可以采用**数字签名**技术；为了验证信息的完**整性和真实性**，可以在信息的后面附加消息鉴别码。

7.身份认证是确认某个实体是**所声称**的实体的行为，根据被认证实体的不同，身份认证包括两种情况：第一种是计算机认证人的身份，称之为用户认证；第二种是**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。指纹锁是基于**生物特征**的用户认证。

8.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。通过 X.509 数字证书中的**签名**可以验证 CA 签名证书的合法性，用证书主体的公钥信息加密的信息只能由**相应的私钥**解密。

9.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。Linux 操作系统采用**自主**访问控制策略，多级安全(multilevelsecure, MLS)是一种**强制**访问控制策略。具有大量（10000 以上）用户的 Web 应用系统应该选用**基于角色**的访问控制策略。

10.空域**隐写术**和**数字水印**方法是 2 类典型的信息隐藏技术，离散余弦变换(DCT)是（ ）方法，离散小波变换(DWT)是（ ）方法。信息隐藏技术的**嵌入强度**越高，鲁棒性就越低。

11.Windows 和 Linux 系统达到了 TCSEC 的 **C2** 安全级别；安全操作系统的安全核是操作系统中与**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。TCB 在 TCSEC 中的定义是：一个计算机系统中的**保护机制**的全体。

12.网络病毒主要包括**网络蹊点**和**网络扫描、查点** 2 个过程。通过向目标程序的缓冲区写超出其长度的内容，可以造成缓冲区的**溢出**。如果目标系统的栈**不可执行**，则缓冲区溢出漏洞**无法被利用**。

13.为了使局域网内的主机共享一个 IP 地址访问因特网，可以采用 **NAT** 技术；为了保证远程主机到内网的安全访问，可以使用 **PPTP** VPN；为了保证两个局域网穿过因特网进行安全互联，可以使用 **L2TP** VPN。

14.按照数据来源分类，入侵检测分为 3 类：**基于主机的入侵检测系统、基于网络的入侵检测系统**和**混合式入侵检测系统**。根据检测方法，入侵检测主要分为**异常检测**和**误用检测**。

15.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**。

16.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。

17.**传染性（自我复制）和破坏性**是计算机病毒的最基本特征。病毒检测技术主要包括**恶意代码静态分析**判定技术和**恶意代码动态分析**判定技术。

18.**简述网络银行保证其根证书可信的一种方法。**
查看颁布的机构是否有相应的资质。

19.**简述信息加密与信息隐藏的主要区别。**
信息加密利用密钥把信息变换成密文，通过公开信道传输。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的事实。其主要目的并不是限制对信息的访问，而是确保信息在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

20.**解释计算机病毒和蠕虫的主要区别。**
病毒需要借助活动的宿主程序或已被感染的活动操作系统才能运行，造成破坏并感染其他可执行文件或文档。病毒侵入系统后，会保持休眠状态，直到被感染的宿主文件或程序被激活，反过来再激活病毒，使其能够在您的系统上运行和复制。
蠕虫是独立的恶意程序，可以通过计算机网络进行自我复制和传播，不需要人工干预。一旦蠕虫侵入系统（通常通过网络连接或以下载的文件形式），就会立即自行创建多个副本，并通过网络或互联网连接传播，感染网络上任何没有得到充分保护的计算机和服务器。网络蠕虫的每个后续副本也可以自我复制，因此可以通过互联网和计算机网络非常迅速地传播感染。

21.**简述信息安全中的机密性、完整性和可用性。**
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】
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】
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，信息系统的服务功能维持运行。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。是信息资源服务功能和性能可靠性的度量】

课后习题

1.**简述拒绝服务攻击和缓冲溢出攻击，论述二者破坏了哪些信息安全属性。**
拒绝服务攻击【攻击者设法让目标系统停止提供服务或资源访问，从而阻止授权实体对系统的正常使用或管理。破坏了可用性】
缓冲溢出攻击【攻击者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，以达到攻击的目的。破坏了完整性】

2.**一个密码系统包括哪些要素？**
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 $e_k \in E$ 和一个解密算法 $d_k \in D$，使得对任意 m∈P，恒有 $d_k(e_k(m))=m$

3.**RSA 算法的理论基础是什么？简述 RSA 算法的流程。**
RSA 算法的理论基础是数论中“大整数的素因子分解是困难问题”的结论，即求两个大素数的乘积在计算机上是容易实现的，但要将一个大整数分解成两个大素数却是困难的。
密钥计算方法：1.选择两个大素数 p 和 q；2.计算 n=pq 和 z=(p-1)(q-1)；3.选择一个与 z 互质的数 d；4.找到一个数 e 使其满足 ed=1(mod z)；5.公开密钥为(e, n)，私有密钥为(d, n)
加密算法：1.将明文视为比特串，将明文划分为长为 k 位的块 p；2.对每个数据块 p，计算 c=p^e(mod n)，c 即为 p 的密文
解密算法：对每个密文块 c，计算 p=c^d(mod n)，p 即为明文

4.**数字签名与消息鉴别的主要区别是？**
应用目的不同：数字签名为防止通信双方的相互欺骗与抵赖行为，可以解决通信双方的内部相互攻击。消息鉴别为证实收到的消息来自可信源点且未被篡改的过程。主要检测的是消息的真实性和完整性，不能处理通信双方的内部相互攻击。
密码体制不同：数字签名属于非对称密码体制，而消息认证码属于对称密码体制，所以消息认证码的处理速度也会比数字签名快很多，但是消息认证码无法实现不可否认性。

5.**计算机系统对人进行认证的主要方法有哪些？**
依据所知道的信息（基于口令的认证），比如身份证号码、账号密码、口令等；依据所拥有的物品（基于智能卡的认证），比如 IC 卡、USBKey 等；依据所具有的独一无二的身体特征（基于生物特征的认证），比如指纹、虹膜、声音等。

6.**什么是数字证书？数字证书的基本功能是什么？**
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。
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。

7.**简述主要的 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，是 PKI 系统整个网络结构的基础。
层次模型：层次结构可以被描绘为一棵倒立的树。在这棵倒立的树上，根代表根 CA，是整个 PKI 的信任锚，所有实体都信任它。根 CA 一般不直接给终端用户颁发证书，而是让证直接连接在它下面的 CA，每个 CA 都认证零个或多个直接连接在它下面的 CA，例数第二层的 CA 认证终端用户。在这种模型中，认证方只需验证从根 CA 到认证节点的这条路径就可以了，不需要建立从根节点到发起认证方的路径。
交叉模型：在这种模型中，如果没有命名空间的限制那么任何 CA 都可以对其他的 CA 发证。所以这种结构非常适合动态变化的组织结构。但是在构建有效的认证路径时，很难确定一个 CA 是否是另一个 CA 的适当证书颁发者。
混合模型：混合模型是将层次结构和交叉结构相混合而得到的模型。其特点是：存在多个根 CA，任意两个根 CA 间都要交叉认证；每个层次结构都在根级有一个单一的交叉证书通向另一个层次结构。
桥 CA 模型：桥 CA 模型实现了一个集中的交叉认证中心，它的目的是提供交叉证书而不是作为证书路径的根。
信任链模型：同时拥有多个根 CA，这些可信的根 CA 被预先提供给客户端系统，为了成功地被验证，证书一定要直接或间接地与这些可信根 CA 连接。

8.**什么是授权？什么是控制访问？**
授权【给已通过认证的用户授予相应的权限。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】

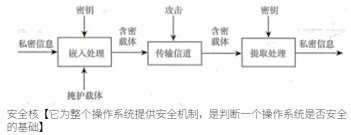
9.**自主控制访问的基本思想是什么？**
客体的所有者（ 或控制者） 对自己的客体进行管理，由所有者决定是否将自己客体的访问权或部分访问权授予其他主体。基于主体的身份和先行规定的访问规则来对访问进行控制。客体的主人全权管理有关该客体的访问授权

10.**强制控制访问的主要特点是什么？**
是权威制定访问规则，对所有主体及其所控制的客体实施强制访问控制。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

11.**RBAC 的基本思想是什么？**
基本思想为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。核心思想是将权限与角色联系起来。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。

12.**简述数字隐写的基本模型。**

13.**什么是 TCB？ 主要包括哪些成分？**
TCB 在 TCSEC 中的定义【一个计算机系统中的保护机制的全体】
固件和硬件【包括 CPU、内存、寄存器和 I/O 设备等，为了保证系统的安全性，这些部分必须能够可信地完成它们的设计任务】
与安全策略相关的文件【比如安全策略库、标识与鉴别的数据库等】
负责安全管理的人员【他们一般具有比较大的权限，所以很容易引起系统的安全问题】



安全核【它为整个操作系统提供安全机制，是判断一个操作系统是否安全的基础】
具有特权的进程或命令

14.**什么是最小特权原则？**
最小特权指的是在完成某种操作时授予每个主体必不可少的特权。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。

15.**什么是 LKM 机制？**
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。系统调用 create_module、init_module、query_module 以及 delete_module 等分别用于创建、初始化、查寻和删除模块。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。

16.**在 CSA 云安全模型中，云存储安全机制主要有哪些方面？**
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】
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】
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】

17.**可信计算的基本思想是什么？**
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保障确保。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

18.**简述常见的拒绝服务攻击方法的原理**
拒绝服务攻击【攻击者设法让目标系统停止提供服务或资源访问，从而阻止授权实体对系统的正常使用或管理。破坏了可用性】
SYN 泛洪攻击【利用 TCP 缺陷，发送大量伪造的 TCP 连接请求，TCP 连接无法完成第三步握手，使被攻击主机的资源耗尽(CPU 满负荷或内存不足)而停止服务】
UDP 泛洪攻击【利用简单的 TCP/IP 服务，如字符发生器协议(chargen)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。这样就在两台主机之间存在很多的无用数据流，这些无用数据流会导致针对带宽服务的攻击】
Ping 泛洪攻击【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】
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】
Land 攻击【原理是设计一个特殊的 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】
Smurf 攻击【通过向一个局域网的广播地址发出 ICMP 回应请求，并将请求的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，最终导致目标主机崩溃】
分布式拒绝服务攻击【借助于客户/服务器技术，将多台主机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力】

19.**防火墙采用了哪些常见的技术？**
服务控制【决定哪些 Internet 服务可以被访问，无论这些服务是从内而外还是从外而内】
方向控制【决定在哪些特定的方向上服务请求可以被发起并通过防火墙】
用户控制【根据用户正在试图访问的服务器，来控制其访问】
行为控制【控制一个具体的服务怎样被实现】

20.**简述包过滤防火墙的工作原理。**
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。具体实现为 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

21.**异常检测和误用检测的基本思想有什么不同？**
异常检测的基本思想是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。相当于建立一个主体正常活动的模型，不符合此模型就警告，类似于白名单。
误用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。相当于建立一个主体异常活动的模型，只有符合此模型才会警告，类似于黑名单。

22.**蜜罐的功能是什么？**
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），诱使攻击者对它们实施攻击，从而可以对攻击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。

23.**安全服务和安全机制的区别和联系是什么？**
联系：安全服务通过安全机制来实现安全策略。
区别：安全服务是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。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。

24.**简述 IPSec 的两种工作模式**
传输模式【主要为直接运行在 IP 层之上的协议，如 TCP、UDP 和 ICMP，提供安全保护，一般用于在两台主机之间的端到端通信】
隧道模式【对整个 IP 包提供保护。为了达到这个目的，当 IP 数据包附加了 AH 或 ESP 域之后，整个数据包加安全域被当做一个新 IP 包的载荷，并拥有一个新的外部 IP 头。一般用于两个网络之间的通信】

25.**802.11i 的认证过程包括哪些阶段？**
802.1x 的认证模型包含三个实体：请求者：STA、认证者：AP、认证服务器。
连接到 AS【STA 向它的 AP 发送一个请求以连接到 AS。AP 识别这个请求并给 AS 发送一个访问请求】
EAP 交换【这个交换让 STA 和 AS 相互授权】
安全密钥分发【一旦认证完成，AS 和 STA 产生一个主会话密钥，此密钥也被称为 AAA 密钥。STA 和 AP 进行安全通信所需的加密密钥都从 MSK 产生】

```
char Lbuffer[] = "0123456789012345678========ABCD";
#define ATTACK_BUFF_LEN 1024
char attackStr[ATTACK_BUFF_LEN];
void foo()
{
    char buff[16];
    strcpy (buff, attackStr);
}
void justCopyTheLbuffer()
{
    strcpy(attackStr, Lbuffer);
}
int main(int argc, char * argv[])
{
    justCopyTheLbuffer(); foo(); return 0;
}
```

反汇编 main 和 foo：

```
(gdb) disas main
Dump of assembler code for function main:
   0x08048534 <+0>: lea 0x4(%esp),%ecx
   0x08048538 <+4>: and $0xfffffff0,%esp
   0x0804853b <+7>: pushl -0x4(%ecx)
   0x0804853e <+10>: push %ebp
   0x0804853f <+11>: mov %esp,%ebp
   0x08048541 <+13>: push %ecx
   0x08048542 <+14>: sub $0x4,%esp
   0x08048545 <+17>: call 0x80484ad <justCopyTheLbuffer>
   0x0804854a <+22>: call 0x804846b <foo>
   0x0804854f <+27>: mov $0x0,%eax
   0x08048554 <+32>: add $0x4,%esp
   0x08048557 <+35>: pop %ecx
   0x08048558 <+36>: pop %ebp
   0x08048559 <+37>: lea -0x4(%ecx),%esp
   0x0804855c <+40>: ret
End of assembler dump.
(gdb)
(gdb) disas foo
Dump of assembler code for function foo:
   0x0804846b <+0>: push %ebp
   0x0804846c <+1>: mov %esp,%ebp
   0x0804846e <+3>: sub $0x18,%esp
   0x08048471 <+6>: sub $0x8,%esp
   0x08048474 <+9>: push $0x804a0a0
   0x08048479 <+14>: lea -0x18(%ebp),%eax
   0x0804847c <+17>: push %eax
   0x0804847d <+18>: call 0x8048320 <strcpy@plt>
   0x08048482 <+23>: add $0x10,%esp
   0x08048485 <+26>: nop
   0x08048486 <+27>: leave
   0x08048487 <+28>: ret
End of assembler dump.
```

设置断点： 在函数 foo 的入口、 对 strcpy 的调用、 出口及其它需要重点分析的位置设置断点。

```
(gdb) b *(foo+0)
Breakpoint 1 at 0x804846b
(gdb) b *(foo+18)
Breakpoint 2 at 0x804847d
(gdb) b *(foo+28)
Breakpoint 3 at 0x8048487
(gdb) display/i $eip
```

运行程序并在断点处观察寄存器的值

```
(gdb) r
Starting program: /home/i/work/buf
Breakpoint 1, 0x0804846b in foo ()
1: x/i $pc
=> 0x804846b <foo>: push %ebp
(gdb) x/x $esp
0xbffff2c:      0x0804854f
(gdb) x/i 0x0804854f
0x804854f <main+27>:    mov $0x0,%eax
```

函数入口处的堆栈指 esp 指向的栈（地址为 **0xbffff2c**）保存了函数 foo() 返回到调用函数(main)的地址（0x804854f），即“函数的返回地址”。记录堆栈指针 esp 的值，在此以 A 标记：**A=$esp=0xbffff2c**

继续执行到下一个断点

```
(gdb) c
Continuing.
Breakpoint 2, 0x0804847d in foo ()
1: x/i $pc
=> 0x804847d <foo+18>:call 0x8048320 <strcpy@plt>
(gdb)
(gdb) x/x $esp
0xbffff00 :      0xbfffef10
(gdb)
0xbffff04 :      0x0804a0a0
(gdb) x/x 0x0804a0a0
0x804a0a0 <attackStr>: 0x33323130
(gdb)
```

查看执行 strcpy(des, src)之前堆栈的内容。由于 C 语言默认将参数逆序推入堆栈，因此，src（第二个参数的地址）先进栈（高地址），des（第一个参数的地址）后进栈（低地址）。可见，attackStr（src）的地址 0x0804a0a0 保存在地址为 0xbffff04 的栈中。buff（des）的首地址 0xbffef10 保存在地址为 0xbffff00 的栈中。
令 **B= buff 的首地址=0xbffef10**， 则 **buff 的首地址与返回地址所在栈的距离=A-B= 0xbffff2c - 0xbffef10=0x1c=28**。因此，如果 attackStr 的内容超过 28 字节，则将发生缓冲区溢出，并且返回地址被改写。attackStr 的长度为 32 字节，其中最后的 4 个字节为“ABCD”。因此，执行 strcpy(des, src)之后，返回地址由原来的 0x0804854f 变为“ABCD”（0x44434241），即返回地址被改写。

继续执行到下一个断点：

```
(gdb) c
Continuing.
Breakpoint 3, 0x08048487 in foo ()
1: x/i $pc
=> 0x8048487 <foo+28>: ret
```

即将执行的指令为 ret。 执行 ret 等价于以下三条指令：eip 的值=esp 指针指向的堆栈内容、跳转到 eip 执行指令、esp=esp+4

```
(gdb) x/x $esp
0xbffff2c: 0x44434241
```

可见，执行 ret 之前的堆栈的内容为“ABCD”，即 0x44434241。可以推断执行 ret 后将跳到地址 0x44434241 去执行。

继续单步执行下一条指令：

```
(gdb) si
0x44434241 in ?? ()
1: x/i $pc
=> 0x44434241:    <error: Cannot access memory at address
0x44434241>
(gdb) x/x $eip
0x44434241:    Cannot access memory at address 0x44434241
(gdb)
```

可见程序指针 eip 的值为 0x44434241，而 0x44434241 是不可访问的地址，因此发生段错误。**eip=0x44434241.** 正好是“ABCD”倒过来，这是由于 IA32 默认字节序为 little_endian（小端字节序， 低字节存放在低地址）

Windbg 命令：
dd ：双字值(4 字节) 默认的显示数量为 32 个 DWORD(128 字节)。每个显示行都会显示行中第一个数据的地址，后面数据的地址依次加 4.