信息安全概论习题参考答案

第 1 章 概论

1. 什么是信息技术?

答：笼统地说，信息技术是能够延长或扩展人的信息能力的手段和方法。

本书中，信息技术是指在计算机和通信技术支持下，用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频以及语音信息，并且包括提供设备和信息服务两大方面的方法与设备的总称。

也有人认为信息技术简单地说就是 3C：Computer＋Communication＋Control。

2. 信息安全的基本属性主要表现在哪几个方面?

答：（1）完整性（Integrity）

（2）保密性（Confidentiality）

（3）可用性（Availability）

（4）不可否认性（Non-repudiation）

（5）可控性（Controllability）

3. 信息安全的威胁主要有哪些?

答：

（1）信息泄露

（2）破坏信息的完整性

（3）拒绝服务

（4）非法使用（非授权访问）

（5）窃听

（6）业务流分析

（7）假冒

（8）旁路控制

（9）授权侵犯

（10）特洛伊木马

（11）陷阱门

（12）抵赖

（13）重放

（14）计算机病毒

（15）人员不慎

（16）媒体废弃

（17）物理侵入

（18）窃取

（19）业务欺骗等

第一章

1、结合实际谈谈你对“信息安全是一项系统工程”的理解。

答:该题为论述题,需要结合实际的信息系统,根据其采取的安全策略和防护措施展开论述。

2、当前信息系统面临的主要安全威胁有哪些?

答：对于信息系统来说，安全威胁可以是针对物理环境、通信链路、网络系统、操作系统、应用系统以及管理系统等方面。通过对已有的信息安全事件进行研究和分析，当前信息系统面临的主要安全威胁包括：信息泄露、破坏信息的完整性、非授权访问（非法使用）、窃听、业务流分析、假冒、网络钓鱼、社会工程攻击、旁路控制、特洛伊木马、抵赖、重放、计算机病毒、人员不慎、媒体废弃、物理侵入、窃取、业务欺骗等。

3、如何认识信息安全“三分靠技术，七分靠管理”?

答：该题为论述题，可以从人事管理、设备管理、场地管理、存储媒介管理、软件管理、网络管理、密码和密钥管理等方面展开论述。

第 2 章 信息保密技术

1. 密码学发展分为哪几个阶段？各自的特点是什么？

答：第一个阶段:从几千年前到 1949 年。

古典加密

计算机技术出现之前

密码学作为一种技艺而不是一门科学

第二个阶段：从 1949 年到 1975 年。

标志：Shannon 发表“Communication Theory of Secrecy System”

密码学进入了科学的轨道

主要技术：单密钥的对称密钥加密算法

第三个阶段：1976 年以后

标志：Diffie，Hellman 发表了“New Directions of Cryptography”

开创了公钥密码学的新纪元。

2. 设计分组密码的主要指导原则是什么？实现的手段主要是什么？

答：a.为了保证密码的安全性，Shannon 提出的混乱原则和扩散原则。

b. 针对实现的设计原则,分组密码可以用软件和硬件来实现。基于软件和硬件的不同性质，分组密码的设计原则可根据预定的实现方法来考虑。

软件实现的设计原则：使用子块和简单的运算。密码运算在子块上进行，要求子块的长度能自然地适应软件编程，比如 8、16、32 比特等。在软件实现中，按比特置换是难于实现的，因此我们应尽量避免使用它。子块上所进行的一些密码运算应该是一些易于软件实现的运算，最好是用一些标准处理器所具有的一些基本指令，比如加法、乘法和移位等。

硬件实现的设计原则：加密和解密可用同样的器件来实现。尽量使用规则结构，因为密码应有一个标准的组件结构以便其能适应于用超大规模集成电路实现。

另外，简单性原则，必要条件，可扩展性也是要考虑的。

c.多数分组密码算法的思想采用了 Feistel 密码结构，用代替和置换的手段实现混淆和扩散的功能。

3. 公钥密码体制出现有何重要意义？它与对称密码体制的异同有哪些？

答： 公钥密码体制是密码学研究的一个具有里程碑意思的重要事件。公钥密码系统在消息的传输过程中采用彼此不同的加密密钥与解密密钥，并且在考虑时间因素的情况下，由加密密钥推导出与之相对应的解密密钥不具有可实现性。至此，密码体制解脱了必须对密钥进行安全传输的束缚，使密码学的应用前景豁然开朗。

与对称密码相比，

相同点：

都能用于数据加密；

都能通过硬件实现；

不同点：

对称密码体制加密密钥和解密密钥是相同的,而公钥密码体制使用不同的加密密钥和解密密钥；

公钥密码体制基于数学难题，而对称密码体制不是；

公钥密码体制密钥分发简单。加密密钥可以做成密钥本公开，解密密钥由各用户自行掌握，而对称密码体制不可以；

公钥体制的加密速度比较慢，而对称密码体制速度较快；

公钥体制适应于网络的发展，能够满足不相识的用户之间进行保密通信的要求；

公钥体制中每个用户秘密保存的密钥量减少。网络中每个用户只需要秘密保存自己的解密密钥，与其他用户通信所使用的加密密钥可以由密钥本得到；

4. 在 DES 算法中，S-盒的作用是什么？

答：每个 S-盒将 6 位输入变成 4 位的输出。它是非线性的，决定了 DES 算法的安全性。

5. 你认为 AES 比 DES 有哪些优点？

答：（1）AES 的密钥长度可以根据需要而增加，而 DES 是不变的；

(2)Rijndael 加解密算法中，每轮常数的不同消除了密钥的对称性，密钥扩展的非线性消除了相同密钥的可能性；加解密使用不同的变换，消除了在 DES 里出现的弱密钥和半弱密钥存在的可能性；总之，在 Rijndael 的加解密算法中，对密钥的选择没有任何限制。

(3)依靠有限域/有限环的有关性质给加密解密提供了良好的理论基础，使算法设计者可以既高强度地隐藏信息，又同时保证了算法可逆，又因为 Rijndael 算法在一些关键常数（例如：在 $m(x)$）的选择上非常巧妙，使得该算法可以在整数指令和逻辑指令的支持下高速完成加解密。

（4）AES 安全性比 DES 要明显高。

10. 现实中存在绝对安全的密码体制吗？

答：否。

11. 信息隐藏和数据加密的主要区别是什么？

答：区别：

目标不同：加密仅仅隐藏了信息的内容； 信息隐藏既隐藏了信息内容，还掩盖了信息的存在。

实现方式不同：加密依靠数学运算；而信息隐藏充分运用载体的冗余空间。

应用场合不同:加密只关注加密内容的安全,而信息隐藏还关注载体与隐藏信息的关系。

联系：

理论上相互借用，应用上互补。信息先加密，再隐藏

12. 信息隐藏的方法主要有哪些？

答：空间域算法与变换域算法。

第二章

1、古典密码技术对现代密码体制的设计有哪些借鉴？

答：一种好的加密法应具有混淆性和扩散性。混淆性意味着加密法应隐藏所有的局部模式，将可能导致破解密钥的提示性信息特征进行隐藏；扩散性要求加密法将密文的不同部分进行混合，使得任何字符都不在原来的位置。古典密码中包含有实现混淆性和扩散性的基本操作：替换和置乱，这些基本操作的实现方式对现代密码体制的设计具有很好的借鉴作用。

2、衡量密码体制安全性的基本准则有哪些？

答：衡量密码体制安全性的基本准则有以下几种：

（1）计算安全的：如果破译加密算法所需要的计算能力和计算时间是现实条件所不具备的，那么就认为相应的密码体制是满足计算安全性的。这意味着强力破解证明是安全的。

（2）可证明安全的：如果对一个密码体制的破译依赖于对某一个经过深入研究的数学难题的解决，就认为相应的密码体制是满足可证明安全性的。这意味着理论保证是安全的。

（3）无条件安全的：如果假设攻击者在用于无限计算能力和计算时间的前提下，也无法破译加密算法，就认为相应的密码体制是无条件安全性的。这意味着在极限状态上是安全的。

3、谈谈公钥密码在实现保密通信中的作用。

答：基于对称密码体制的加密系统进行保密通信时，通信双方必须拥有一个共享的秘密密钥来实现对消息的加密和解密，而密钥具有的机密性使得通信双方如何获得一个共同的密钥变得非常困难。而公钥密码体制中的公开密钥可被记录在一个公共数据库里或者以某种可信的方式公开发放，而私有密钥必须由持有者妥善地秘密保存。这样，任何人都可以通过某种公开的途径获得一个用户的公开密钥，然后与其进行保密通信，而解密者只能是知道相应私钥的密钥持有者。用户公钥的这种公开性使得公钥体制的密钥分配变得非常简单，目前常用公钥证书的形式发放和传递用户公钥，而私钥的保密专用性决定了它不存在分配的问题，有效解决了保密通信中的密钥管理问题。公约密码体制不仅能够在实现消息加解密基本功能的同时简化了密钥分配任务，而且对密钥协商与密钥管理、数字签名与身份认证等密码学问题产生了深刻的影响。

4、验证 RSA 算法中解密过程的有效性。

证明： 数论中的欧拉定理指出，如果两个整数 a 和 b 互素，那么 $a^{\varphi(b)} \equiv 1 \bmod b$ 。

在 RSA 算法中，明文 m 必与两个素数 p 和 q 中至少一个互素。不然的话，若 m 与 p 和 q 都不互素，那么 m 既是 p 的倍数也是 q 的倍数，于是 m 也是 n 的倍数，这与 $m < n$ 矛盾。

由 $de \equiv 1 \mod \phi(n)$ 可知存在整数 k 使得 $de = k\phi(n) + 1$ 。下面分两种情形来讨论：

情形一：m 仅与 p 、q 二者之一互素，不妨假设 m 与 p 互素且与 q 不互素，那么存在整数 a 使得 $m = aq$ ，由欧拉定理可知

$$m^{k\varphi(n)} \bmod p \equiv m^{k\varphi(p)\varphi(q)} \bmod p \equiv (m^{\varphi(p)})^{k\varphi(q)} \bmod p \equiv 1 \bmod p$$

于是存在一个整数 t 使得 $m^{k\phi(n)} = tp + 1$ 。给 $m^{k\phi(n)} = tp + 1$ 两边同乘以 $m = aq$ 得到

$$m^{k\phi(n)+1} = tapq + m = tan + m$$

由此得 $c^d = m^{ed} = m^{k\phi(n)+1} = tan + m \equiv m \mod n$ 。

情形二：如果 m 与 p 和 q 都互素，那么 m 也和 n 互素，我们有

$$c^d = m^{ed} = m^{k\varphi(n)+1} = m \times m^{k\varphi(n)} \equiv m \bmod n \text{ 。}$$

第三章 信息认证技术

1. 简述什么是数字签名。

答：数字签名就是通过一个单向函数对要传送的报文进行处理得到的用以认证报文来源并核实报文是否发生变化的一个字母数字串，该字母数字串被成为该消息的消息鉴别码或消息摘要，这就是通过单向哈希函数实现的数字签名；在公钥体制签名的时候用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据，然后信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，并通过与用自己收到的原始数据产生的哈希摘要对照，便可确信原始信息是否被篡改，这样就保证了数据传输的不可否认性。这是公钥签名技术。

2. 杂凑函数可能受到哪几种攻击？你认为其中最为重要的是哪一种？

答：穷举攻击、生日攻击和中途相遇攻击。

第三章

1、评价 Hash 函数安全性的原则是什么？

答：对于 Hash 函数的安全要求，通常采用原像问题、第二原像问题、碰撞问题这三个问题来进行判断。如果一个 Hash 函数对这三个问题都是难解的，则认为该 Hash 函数是安全的。

2、公钥认证的一般过程是怎样的？

答：发信方 Alice 用自己的私有密钥 sk_A 加密消息 m，任何人都可以轻易获得 Alice 的公开秘密 pk_A，然后解开密文 c，由于用私钥产生的密文只能由对应的公钥来解密，根据公私钥一一对应的性质，别人不可能知道 Alice 的私钥，如果收信方 Bob 能够用 Alice 的公钥正确地还原明文，表明这个密文一定是 Alice 用自己的私钥生成的，因此 Bob 可以确信收到的消息确实来自 Alice，同时 Alice 也不能否认这个消息是自己发送的；另一方面，在不知道发信者私钥的情况下不可能篡改消息的内容，因此收信者还可以确信收到的消息在传输过程中没有被篡改，是完整的。

3、数字签名标准 DSS 中 Hash 函数有哪些作用？

答：通过对消息进行 Hash 计算，可以将任意长度的消息压缩成固定长度的消息摘要，从而提高签名算法的效率，也可以实现对消息完整性的鉴别。

4、以电子商务交易平台为例，谈谈 PKI 在其中的作用。

答：该题为论述题，可以从证书管理、证书应用、安全性等方面展开论述。

5、在 PKI 中，CA 和 RA 的功能各是什么？

答：CA 指认证中心，在 PKI 体系中，认证中心 CA 是整个 PKI 体系中各方都承认的一个值得信赖的、公正的第三方机构。CA 负责产生、分配并管理 PKI 结构下的所有用户的数字证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份，同时 CA 还负责证书废止列表 CRL 的登记和发布。

RA 指注册中心，注册中心 RA 是 CA 的证书发放、管理的延伸。RA 负责证书申请者的信息录入、审核以及证书的发放等任务，同时，对发放的证书完成相应的管理功能。RA 一般都是由一个独立的注册机构来承担，它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。RA 并不给用户签发证书，只是对用户进行资格审查。

第四章 密钥管理技术

1. 什么是密钥托管？

答：密钥托管是指用户在向 CA 申请数据加密证书之前，必须把自己的密钥分成 t 份交给可信赖的 t 个托管人。任何一位托管人都无法通过自己存储的部分用户密钥恢复完整的用户密码。只有这 t 个人存储的密钥合在一起才能得到用户的完整密钥。

第四章

1、结合实际应用，谈谈你对数字水印脆弱性和鲁棒性关系的认识。

答：该题为论述题，可以从鲁棒性要求水印信息对变换不敏感，而脆弱性要求水印信息对变换具有敏感性的角度展开论述。

2、评价隐藏效果的指标有哪些？性能如何？

答：评价隐藏效果的指标有很多，从性能上分，包括以下几个方面：透明性，要求隐藏后的结果图像与原始数据没有明显差别；鲁棒性，要求隐藏的结果数据具有很好的抗变换处理的

性能；安全性，要求隐藏算法具有良好的想安全性等。

第 5 章 访问控制技术

1. 什么是访问控制？访问控制包括哪几个要素？

访问控制是指主体依据某些控制策略或权限对客体本身或是其资源进行的不同授权访问。

访问控制包括三个要素，即：主体、客体和控制策略。

主体：是可以对其它实体施加动作的主动实体，简记为 ***S***。

客体：是接受其他实体访问的被动实体, 简记为 ***O***。

控制策略：是主体对客体的操作行为集和约束条件集, 简记为 ***KS***。

2. 什么是自主访问控制？什么是强制访问控制？这两种访问控制有什么区别？说说看，你会在什么情况下选择强制访问控制。

自主访问控制模型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它用户。

强制访问控制模型是一种多级访问控制策略，它的主要特点是系统对访问主体和受控对象实行强制访问控制，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。

区别：自主访问控制模型中，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；强制访问控制模型中系统事先给访问主体和受控对象分配不同的安全级别属性，通过分级的安全标签实现了信息的单向流通。

强制访问控制一般在访问主体和受控客体有明显的等级划分时候采用。

3. 审计的重要意义在于什么？你通过什么方式来达到审计的目的？除了我们书上讲的内容外，你还能想到其他的审计方式吗？

审计是访问控制的重要内容与补充，审计可以对用户使用何种信息资源、使用的时间以及如何使用进行记录与监控。审计的意义在于客体对其自身安全的监控，便于查漏补缺，追踪异常事件，从而达到威慑和追踪不法使用者的目的。

审计的方式：

基于规则库的方法：将已知的攻击行为进行特征提取，把这些特征用脚本语言等方法进行描述后放入规则库中，当进行安全审计时，将收集到的网络数据与这些规则进行某种比较和匹配操作（关键字、正则表达式、模糊近似度），从而发现可能的网络攻击行为。

基于统计的方法：首先给对象创建一个统计量的描述，比如网络流量的平均值、方差等，同基础正常情况下的这些特征量的数值，然后对实际的网络数据情况进行对比，当发现远离正常值的情况，则可以判断攻击的存在

此外，人工智能、神经网络、数据挖掘等最新相关领域的知识也可不同程度的引入到安全审计中来，为安全审计技术带来新的活力。

第五章

1、操作系统安全机制有哪些？

答：操作系统安全的主要目标是监督保障系统运行的安全性，保障系统自身的安全性，标识系统中的用户，进行身份认证，依据系统安全策略对用户的操作行为进行监控。为了实现这些目标，在进行安全操作系统设计时，需要建立相应的安全机制。常用的安全机制包括：硬件安全机制、标识与认证机制、存取控制机制、最小特权管理机制、安全审计机制等。

2、Windows XP 操作系统的安全机制有哪些？

答：在 Windows XP 操作系统中，安全机制主要由本地安全认证、安全账号管理器和安全参考监督器构成。除此之外，还包括注册、访问控制和对象安全服务等，它们之间的相互作用和集成构成了该操作系统的安全子系统。

3、实现数据库安全的策略有哪些？

答：数据库安全策略是指如何组织、管理、保护和处理敏感信息的原则，它包含以下方面：最小特权策、最大共享策略、粒度适当策略、开放和封闭系统策略、按存取类型控制策略、与内容有关的访问控制策略、与上下文有关的访问控制策略、与历史有关的访问控制策略。

4、库内加密和库外加密各有什么特点？

答：库内加密指在 DBMS（Data Base Management System 数据库管理系统）内部实现支持加密的模块。其在 DBMS 内核层实现加密，加密/解密过程对用户和应用是透明的。数据进入 DBMS 之前是明文，DBMS 在对数据物理存取之前完成加密/解密工作。库内加密通常是以存储过程的形式调用，因为由 DBMS 内核实现加密，加密密钥就必须保存在 DBMS 可以访问的地方，通常是以系统表的形式存在。库内加密的优点是加密功能强，并且加密功能几乎不会影响 DBMS 的原有功能，这一点与库外加密方式相比尤为明显。另外，对于数据库来说，库内加密方式是完全透明的，不需要对 DBMS 做任何改动就可以直接使用。

库外加密指在 DBMS 范围外，用专门的加密服务器完成加密/解密操作。数据库加密系统作为 DBMS 的一个外层工具，根据加密要求自动完成对数据库数据的加密/解密处理。加密/解密过程可以在客户端实现，或者由专业的加密服务器完成。对于使用多个数据库的多应用环境，可以提供更为灵活的配置。

第六章

1、基于角色的访问控制有哪些技术优点？

答：基于角色的访问控制是指在应用环境中，通过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。系统只问用户是什么角色，而不管用户是谁。角色可以理解成为其工作涉及相同行为和责任范围内的一组人。该访问控制模型具有以下特点：便于授权管理、便于赋予最小特权、便于根据工作需要分级、责任独立、便于文件分级管理、便于大规模实现。

2、PKI 与 PMI 的联系和区别是什么？

答：PMI 负责对用户进行授权，PKI 负责用户身份的认证，两者之间有许多相似之处。

AA 和 CA 在逻辑上是相互独立的，而身份证书的建立可以完全独立于 PMI 的建立，因此，整个 PKI 系统可以在 PMI 系统之前建立。CA 虽然是身份认证机构，但并不自动成为权限的认证机构。

PKI 与 PMI 的主要区别如下：

（1）两者的用途不同：PKI 证明用户的身份，PMI 证明该用户具有什么样的权限，而且 PMI 需要 PKI 为其提供身份认证。

（2）两者使用的证书不同：PKI 使用公钥证书，PMI 使用属性证书。

（3）两者的工作模式不同：PKI 可以单独工作，而 PMI 是 PKI 的扩展，PMI 开展工作时依赖 PKI 为其提供身份认证服务。

第 7 章 网络安全技术

1. 什么是防火墙，它应具有什么基本功能？

因特网防火墙是这样的（一组）系统，它能增强机构内部网络的安全性，用于加强网络间的访问控制，防止外部用户非法使用内部网的资源，保护内部网络的设备不被破坏，防止内部网络的敏感数据被窃取。

防火墙的基本功能是对网络通信进行筛选屏蔽以防未经授权的访问进出计算机网络。

2. 防火墙有哪几种体系结构，他们的优缺点是什么，如何合理地选择防火墙体系结构？

（1）双宿主主机防火墙

双宿主主机通过用户直接登录到双宿主主机上来提供服务，从而需要在双宿主主机上开许多帐号，这是很危险的：

（a）用户帐号的存在会给入侵者提供相对容易的入侵通道，每一个帐号通常有一个可重复使用口令（即通常用的口令，和一次性口令相对），这样很容易被入侵者破解。破解密码可用的方法很多，有字典破解、强行搜索或通过网络窃听来获得。

（b）如果双宿主主机上有很多帐号，管理员维护起来是很费劲的。

（c）支持用户帐号会降低机器本身的稳定性和可靠性。

（d）因为用户的行为是不可预知的，如双宿主主机上有很多用户帐户，这会给入侵检测带来很大的麻烦。

（2）被屏蔽主机防火墙

一般说来，路由器只提供非常有限的服务，所以保卫路由器比保卫主机更容易实现，从这一点可以看出，被屏蔽主机结构能提供比双宿主主机更好的安全性和可用性。

但是，如果侵袭者设法侵入堡垒主机，则在堡垒主机和其余内部主机之间没有任何保护网络安全的东西。路由器同样会出现这样的问题，如果路由器被损害，整个网络对侵袭者是开放的。因此，被屏蔽子网体系结构变得日益普及。

（3）被屏蔽子网防火墙

采用了屏蔽子网体系结构的堡垒主机不易被入侵者控制，万一堡垒主机被控制，入侵者仍然不能直接侵袭内部网络，内部网络仍受到内部过滤路由器的保护。

（4）其他形式的防火墙体系结构：将被屏蔽子网结构中的内部路由器和外部路由器合并；屏蔽子网结构中堡垒主机与外部路由器合并；使用多台堡垒主机；使用多台外部路由器；使用多个周边网络。

实际中选择防火墙时，需要平衡安全牢固性和设备条件的限制，以求用最简单的设备实现相对高的安全。

11．什么是网络的物理隔离？

所谓物理隔离，是指内部网络与外部网络在物理上没有相互连接的通道，两个系统在物理上完全独立。要实现外部网与内部网络物理隔离的目的，必须保证做到以下几点：

（1）在物理传导上使内外网络隔断。

（2）在物理辐射上隔断内部网与外部网。

（3）在物理存储上隔断两个网络环境。

4. 威胁信息系统安全的来源有哪几类？

对信息系统安全构成威胁的原因是多方面的，概括地讲,威胁信息网络安全因素的来源有两种途径：

（1） 网络内部因素

主要是指网络内部管理制度不健全或制度执行不力，造成管理混乱，缺乏有效的监测机制，给非授权者以可乘之机进行非法攻击。还包括网络管理人员进行网络管理或网络配置时操作不当。

（2） 网络外部因素

主要有三类群体从外部对信息网络进行威胁和攻击：黑客、信息间谍、计算机罪犯。

第七章

1、防火墙的主要类型有哪些？

答：根据防火墙的工作原理，可以将防火墙分为三种：包过滤防火墙、应用级网关和状态检测防火墙。

2、IDS 的组成部分各有哪些功能？

答：入侵检测系统分为四个组件：事件产生器、事件分析器、响应单元和事件数据库。

事件产生器:入侵检测的第一步就是信息收集,收集的内容包括整个计算机网络中系统、网络、数据及用户活动的状态和行为，这是由事件产生器来完成的。入侵检测在很大程度上依赖于信息收集的可靠性、正确性和完备性。因此，要确保采集、报告这些信息软件工具的可靠性，即这些软件本身应具有相当强的坚固性，能够防止被篡改而收集到错误的信息。否则，黑客对系统的修改可能使系统功能失常但看起来却跟正常的系统一样，也就丧失了入侵检测的作用。

事件分析器：事件分析器是入侵检测系统的核心，它的效率高低直接决定了整个入侵检测系统的性能。事件分析器又可称为检测引擎，它负责从一个或多个探测器处接受信息，并通过分析来确定是否发生了非法入侵活动。分析器组件的输出为标识入侵行为是否发生的指示信号，例如一个警告信号，该指示信号中还可能包括相关的证据信息。另外，分析器还能够提供关于可能的反应措施的相关信息。根据事件分析的不同方式可将入侵检测技术分为异常入侵检测、误用入侵检测和完整性分析三类。

事件数据库：事件分析数据库是存放各种中间和最终数据地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。考虑到数据的庞大性和复杂性，一般都采用成熟的数据库产品来支持。事件数据库的作用是充分发挥数据库的长处，方便其他系统模块对数据的添加、删除、访问、排序和分类等操作。通过以上的介绍可以看到，在一般的入侵检测系统中，事件产生器和事件分析器是比较重要的两个组件，在设计时采用的策略不同，其功能和影响也有很大的区别，而响应单元和事件数据库则相对来说比较固定。

响应单元：当事件分析器发现入侵迹象后，入侵检测系统的下一步工作就是响应。而响应的对象并不局限于可疑的攻击者。

3、VPN 的工作原理是什么？

答：VPN 的基本原理是：在公共通信网上为需要进行保密通信的通信双方建立虚拟的专用通信通道，并且所有传输数据均经过加密后再在网络中进行传输，这样做可以有效保证机密数据传输的安全性。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，虚拟的专用网络通过某种公共网络资源动态组成。

4、病毒有哪些基本特征？

答：所谓计算机病毒是指一种能够通过自身复制传染，起破坏作用的计算机程序。它可以隐藏在看起来无害的程序中，也可以生成自身的拷贝并插入到其他程序中。计算机病毒程序是一种特殊程序，这类程序的主要特征包括：、非授权可执行性、隐蔽性、传染性、潜伏性、表现性或破坏性、可触发性等。

第八章

1、风险评估的基本过程是什么？

答：信息安全风险评估是依照科学的风险管理程序和方法，充分的对组成系统的各部分所面临的危险因素进行分析评价，针对系统存在的安全问题，根据系统对其自身的安需求，提出有效的安全措施，达到最大限度减少风险、降低危害和确保系统安全运行的目的。风险评估的过程包括风险评估准备、风险因素识别、风险程度分析和风险等级评价四个阶段。

2、信息安全管理的指导原则有哪些？

答：信息安全管理的基本原则包括：

（1）以安全保发展，在发展中求安全

（2）受保护资源的价值与保护成本平衡

（3）明确国家、企业和个人对信息安全的职责和可确认性

（4）信息安全需要积极防御和综合防范

（5）定期评估信息系统的残留风险

（6）综合考虑社会因素对信息安全的制约

（7）信息安全管理体现以人为本

3、身份管理模型中，IdP 的作用是什么？

答：IdP 指身份提供方，在身份管理模型中，用户的身份信息是由 IdP 统一管理和认证，各个 SP 的身份服务器负责转发实体的身份标识信息并从 IdP 接收确认信息和临时管理用户相关的身份信息。IdP 与各个 SP 的身份服务器共同组成了一个信任域(COT：Circle of Trust)，身份信息在该信任域内能自由互通。

4、简要说明等级保护的重要性。

答：要实现对信息和信息系统的有效防护，最有效和科学的方法是在维护安全、健康、有序的网络运行环境的同时，以分级分类的方式确保信息和信息系统安全既符合政策规范，又满足实际需求。对信息和信息系统进行分级保护是体现统筹规划、积极防范、重点突出的信息安全保护原则的重大措施。

第九章

1、CC 由哪几部分构成？

答：信息技术安全性评估通用准则（CC：Common Criteria），通常简称通用准则，CC 由一系列截然不同但又相互关联的部分组成，定义了一套能满足各种需求的 IT 安全准则，整个标准分为三部分：

第 1 部分—简介和一般模型，正文介绍了 CC 中的有关术语、基本概念和一般模型以及与评估有关的一些框架，附录部分主要介绍保护轮廓（PP）和安全目标（ST）的基本内容。

第 2 部分—安全功能要求，按“类-子类-组件”的方式提出安全功能要求，每一个类除正文外，还有对应的提示性附录做进一步解释。

第 3 部分—安全保证要求，定义了评估保证级别，建立了一系列安全保证组件作为

表示 TOE 保证要求的准则方法。第 3 部分列出了一系列保证组件、族和类。第 3 部分也定义了 PP 和 ST 的评估准则，并提出了评估保证级别。

2、SSE-CMM 的模型结构是什么？

答：SSE-CMM 的结构被设计以用于确认一个安全工程组织中某安全工程各领域过程的成熟度，这种结构的目标就是将安全工程的基础特性与管理制度特性区分清楚。为确保这种区分，模型中建立了两个维度——“域维”和“能力维”，“域维”包含所有集中定义安全过程的实施，这些实施被称作“基础实施”。“能力维”代表反映过程管理与制度能力的实施。这些实施被称作“一般实施”，这是由于它们被应用于广泛的领域。“一般实施”应该作为执行“基础实施”的一种补充。

3、我国计算机信息系统安全保护等级划分的基本原则是什么？

答：我国计算机信息系统安全保护等级划分的基本原则是：

（1） 组织级别与等级保护的关系：组织的行政级别越高，相应的等级保护级别也越高。

（2） 敏感程度与保护等级的关系：信息系统及其信息的敏感程度越高，相应的等级保护级别也越高。

（3） 敏感信息量与保护等级的关系：相对集中的敏感信息量越大，相应的等级保护级别也越高。

（4） 履行职能与保护等级的关系：职能与国家安全、国计民生、社会稳定的关系越大，相应的等级保护级别也越高。