**第一章知识点**

**1、信息系统安全的基本概念**

* 什么是信息安全？

信息安全是指信息在产生、传输、处理、存储和使用过程中的安全。是为了防止未经授权就对知识、实事、数据或能力进行使用、滥用、修改、破坏、拒绝使用或使信息被非法系统辨识、控制而采取的措施。

信息安全的本质：可信（没有出现未预期的结果）和可控（所有操作在控制范围之内）

信息安全主要包括四个层面：系统安全（信息安全的首要问题）、数据安全、内容安全和行为安全。其中数据安全和内容安全就是传统的信息安全，即狭义信息安全，它强调信息本身的安全属性。

* 什么是信息系统安全？

信息系统是指信息产生、存储、处理、传输和使用的人-机一体化计算机系统，包括：计算机硬件、软件、固件、网络和人员。

信息系统安全是指保证信息系统的硬件、软件或固件、网络不因偶然的或恶意的原因而遭受破坏、更改、访问和泄露，从而保证信息系统能够连续可靠地正常运行，提供稳定的服务。

信息系统安全强调信息系统整体上的安全性，即为运行在其上的系统（应用）、处理的数据和执行的操作（行为）提供一个安全的环境，是信息安全的基础。

信息系统的安全功能分为：物理安全、系统软件安全、网络安全、应用软件运行安全和安全管理。

**2、信息系统的基本安全属性（或安全需求）**

GA/T 708-2007定义的基本属性，也是信息系统安全的目标，美国联邦政府FIPS-199也采用了类似的分类方法。

（1）保密性：保密性是指信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

（2）完整性：完整性指网络信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

（3）可用性：可用性是指信息可被授权实体访问并按需求使用的特性。

国际电信联盟标准ITU-T X.800中，则从信息系统提供安全服务的角度，将信息系统安全需求分为：认证、访问控制、机密性、完整性和不可否认性，这也可以看成是信息在产生、传输、存储、处理和使用等过程中的安全需求。

浓缩成两个：可信和可控。

保护范围：信息系统的物理实体、操作系统、数据库管理系统、网络系统、应用软件系统。

**3、安全风险和安全威胁**

* 系统的脆弱性包含哪些方面？

信息系统的安全风险是“绝对的”，无论是否意识到，安全风险都存在，它与人的行为密切相关。信息系统的任何安全风险或不确定事件都可能造成损失。

信息系统的安全风险主要来源于系统的脆弱性，即安全漏洞，而且这种安全风险是全方位的，动态变化的。

（1）电磁泄露：辐射泄漏、传导泄漏；

（2）芯片的脆弱性：芯片存在设计缺陷、“后门”；

（3）操作系统的安全漏洞：操作系统软件在设计上的缺陷或错误；

（4）数据库的安全漏洞：数据库自身存在安全缺陷、错误部署和配置、SQL注入；

（5）通信协议的安全漏洞：协议的开放性、协议的设计缺陷、代码实现的缺陷；

（6）移动存储介质的安全漏洞：移动存储介质在信息系统之间随意使用，造成病毒感染和传播，将内部介质非法带出使用，造成数据外泄。

* 安全威胁的来源

信息系统安全威胁是指由于信息系统存在软、硬件缺陷，或系统集成缺陷，或软件协议等安全漏洞，以及信息安全管理中潜在薄弱环节，信息系统的组成要素和功能可能遭受破坏或无法实现预期目标的可能性。

信息系统的安全威胁主要来源于自然因素和人为因素。自然因素造成的威胁是一种偶发性威胁，它由不可抗力或偶然性事件构成，具有发生概率小、随机性大的特点，如断电、鼠灾、设备的自然老化、电磁干扰、恶劣的场地环境和地震洪灾等意外事故或自然灾害。

人为因素主要包括：

（1）物理攻击：通过物理接触信息系统及其周边设备的方式，对信息系统的硬件、软件和数据产生破坏。

（2）网络攻击：利用网络设备或协议存在的漏洞或安全缺陷对信息系统的硬件、软件及其数据进行攻击的行为。

（3）恶意代码：指在用户不知情或未授权情况下潜入信息系统，在信息系统上安装运行，对信息系统产生威胁或潜在威胁的计算机代码。

（4）安全管理：指通过维护信息系统的机密性、完整性和可用性等安全需求，指导、规范和管理信息系统的一系列活动和过程。

信息系统安全问题的根源：信息系统的开放性、信息系统的脆弱性、黑客的恶意入侵。

即使信息系统无任何脆弱性，也会受到来自包括自然因素和人为因素的安全威胁，从而带来安全问题。例如，对信息系统的人为电磁干扰，属于人为进行的物理攻击，通过物理接触信息系统以及其周边设备，对信息系统的软硬件和数据进行破坏。

* 安全脆弱性、安全威胁和安全损失（安全事件）三者的关系

风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成安全事件。只有利用了脆弱性的威胁才能对资产造成损失，即导致安全损失（安全事件）。

**第二章知识点**

**1、为什么要研究信息系统安全体系结构**

* 从系统的角度考虑信息安全问题；
* 为安全需求、安全技术方法与安全评估标准、相关法律法规之间架起一座桥梁；
* 安全体系结构能够极大地促进安全系统设计的重用；
* 有利于保障安全系统间的互连、互通、互操作

信息系统安全体系结构是从系统的角度解决信息系统安全问题，将普遍性的安全体系原理与信息系统自身实际应用相结合，形成满足信息系统安全需求的体

系结构。目标：从技术和管理上保证完整准确地实现安全策略，全面准确地满足安全需求。安全需求：安全服务、安全机制、安全技术和技术管理，及它们在系统上的合理部署和关系配置等。

1980年，国际标准化组织（ISO）针对计算机网络体系结构提出了“开放系统互连基本参考模型（OSI/RM）”，并在此基础上提出了开放系统互连的安全体系结构标准ISO 7498-2。

设计信息系统安全的安全保障系统，将协议层次、信息系统构成单元和安全服务（安全机制）作为三维坐标体系的三个维来表示，为信息系统安全提供全面的技术保障。

**2、构成信息系统安全体系结构的要素**

（1）安全需求：安全需求是指信息系统要达到的安全服务要求，是制定安全策略和建立安全模型的前提；

（2）安全策略：安全策略指用于限定一个系统、实体或对象进行安全相关活动的规则集，即要表明在安全范围内什么是允许的，什么是不允许的；

（3）安全模型：安全模型用于准确描述系统在功能和结构上的安全特性，它反映了一定的安全策略，是引导和验证安全系统开发设计的一种概念模型；

（4）安全机制：安全机制是实现信息系统安全需求及安全策略的各种措施，具体可以表现为所需要的安全标准、安全协议、安全技术、安全单元等。

\* 四种安全体系结构类型

（1）抽象体系：从描述需求开始，定义执行这些需求的功能函数。之后定义如何选用这些功能函数，以及如何把这些功能组织成一个整体的原理和相关的基本概念。

（2）通用体系：通用安全体系是在已有的安全功能和相关安全服务配置的基础上，定义系统分量类型及实现这些安全功能的有关安全机制。

（3）逻辑体系：逻辑体系就是满足某个假设需求集合的一个设计，它显示了把一个通用体系应用于具体环境时的基本情况。

（4）特殊体系：表达系统分量、接口、标准、性能和开销，表明如何把所有信息安全分量和机制结合起来以满足我们正在考虑的特殊系统的安全需求。

**3、安全体系结构的设计原则**

（1）从系统设计之初就考虑安全性

系统设计时，可以达到系统要求的方法是多种多样的，有的对安全有利，有的对安全不利。在这种情况下，如果没有一个安全体系结构来指导系统设计的早期决策，就完全有可能选择了有致命安全缺陷的设计思路，从而只能采取在系统设计完成后，再添加安全功能补救措施，但此时可能需要付出比选择其他方案要多很多倍的代价才能获得相应的安全特性和保证。

（2）应尽量考虑未来可能面临的安全需求

着眼未来，尽量将不在计划之列的潜在安全属性考虑在内。

原因：实现系统安全增强有两个途径：改进系统原有的安全性；给系统增加新的安全属性。

问题：前者，有时无法改进；后者，系统无法按照希望方式工作。

如何预设安全问题：预设安全问题不能太特殊或太具体；从抽象层次理解安全问题，而不是针对具体的问题；特别关注安全策略的制定。一旦改变，可能对系统造成灾难性的影响。

（3）实现安全控制的极小化和隔离性

极小化系统内部安全部分的复杂度和规模尺度；在系统设计时，确保安全控制的隔离性。作用：添加新的、有用的安全属性时，系统可靠性不改变。

注意事项：

不是任何有效的设计原则都适合安全部分的设计，如：经济性原则；安全机制应尽量简洁、独立；数据隔离必须适度，不能极端。

（4）实施极小特权

与隔离安全机制紧密相关。基本点：在执行某个操作，其进程（主体）除了能够获得执行该操作所需要的权限外，不得获得其他权限。

硬件特权、软件特权、最小特权的实施方法、最小特权总是包含用户的行为和系统管理者的行为。

（5）安全相关功能必须结构化

从而比较容易地确定系统安全相关的内容；需要制定规范的结构。

（6）使安全性能友好

遵循的原则：安全不应当对服从安全规则的用户造成功能影响；授权用户访问应该是容易的；限制用户访问应该是容易的；建立合理的默认规则。

（7）使安全性不依赖于保密

系统的安全体系要避免依赖于系统安全机制的任何保密部分。例如：用户不能突破系统，不能因为用户没有用户手册或软件资源列表。

**4、安全体系结构的发展历程**

（1）1960s-1970s无安全体系结构阶段

《可信计算机系统评估准则》以经典安全模型为基础实现计算机系统安全，是目前公认的信息系统安全体系结构的最早标准。

（2）1980s-1990s安全体系结构初级阶段

1989年ISO 7498-2首次提出“安全体系结构”。

（3）1990s-2000s安全体系结构发展阶段

出现了大量不同类型的信息系统安全体系结构，如：DTOS、Flask、DOCT等，强调：严防死守。

（4）2000-至今安全体系结构高级阶段

信息系统网络化。边界模糊，以防火墙技术为中心的传统安全防护手段不再适用，需要全新的信息安全理念和架构。代表事件：IATF3.0。

强调：保护、检测、反应和恢复；要保证信息系统在遭受攻击的情况下，能够及早地识别、检测出这些攻击，将可能造成的损失降到最低程度，并保证信息系统基本业务的连续性。

**5、ISO安全体系结构解决的安全问题及其服务形式和安全机制**

目的是允许异构计算机系统互联，使得应用进程间的有用通信可达，而为了保护应用进程间交换信息，必须建立系统的安全性。其核心内容是尽可能地将安全服务（即身份认证、访问控制、数据保密、数据完整性、抗否认性等5大类安全服务）与安全机制（即加密、数字签名、访问控制、数据完整性、鉴别交换、通信业务填充、路由选择控制、公证等8类安全机制）放置于OSI模型的7层协议中，以实现端系统信息传送的安全通信通路，这是目前网络安全研究中主要参考的安全体系结构之一。

五大类安全服务

（1）身份认证服务：提供对通信中对等实体和数据来源的认证。

（2）访问控制服务：对资源提供保护，以对抗其非授权使用和操纵。

（3）数据保密服务：保护信息不被泄露或暴露给未授权的实体。

（4）数据完整性服务：对数据提供保护，以对抗未授权的改变、删除和替换。

（5）抗否认性服务：防止参与某次通信、交换信息的任何一方事后否认本次通信或通信内容。

OSI安全服务与服务形式

|  |  |
| --- | --- |
| **安全服务** | **服务形式** |
| 身份认证 | 对等实体认证 |
| 数据源认证 |
| 访问控制 | 访问控制 |
| 数据保密 | 连接保密性 |
| 无连接保密性 |
| 选择字段保密性 |
| 通信业务流保密性 |
| 数据完整性 | 有恢复的连接完整性 |
| 无恢复的连接完整性 |
| 选择字段连接完整性 |
| 无连接完整性 |
| 选择字段无连接完整性 |
| 不可否认性 | 源发方抗抵赖 |
| 接收方抗抵赖 |

8类安全机制

（1）加密机制：加密既能为数据提供保密性，也能为通信业务流提供保密性，并且还能为其它机制提供补充；

（2）数字签名机制：可以完成对数据单元的签名工作，也可实现对已有签名的验证工作；

（3）访问控制机制：按实体所拥有的访问权限对指定资源进行访问，对非授权或非法访问应有报警或审计跟踪方法；

（4）数据完整性机制：针对数据单元，发送方产生一个与数据单元相关的附加码，接收方通过对数据单元与附加码的验证；

（5）鉴别交换机制：使用密码技术，由发送方提供，而由接收方验证来实现鉴别。通过特定的“握手”协议防止鉴别“重放”；

（6）通信业务填充机制：业务分析，特别是基于流量的业务分析是攻击通信系统的主要方法之一；

（7）路由选择控制机制：针对数据单元的安全性要求，可以提供安全的路由选择方法；

（8）公证机制：通过第三方机构，实现对通信数据的完整性、原发性、时间和目的地等内容的公证。

开放系统网络互联安全体系结构在实际应用中，协议每一层都可以提供端对端加密机制。物理层需确保安全的物理信道，数据链路层需给传输链路加密，网络层需要采用防火墙，防止病毒入侵等，传输层需要进行端对端加密。

**6、几种典型安全体系结构之间的区别**

（1）基于协议的安全体系结构

协议是网络的同一层次实体之间、为了相互配合完成本层次功能的约定，所以，协议是网络体系结构的最终体现形式。基于协议的安全体系结构而言，它的基本构成成分和最终体现形式就是网络安全协议。

基于TCP/IP协议的安全体系结构是基于协议安全体系结构中重要组成部分，包括提供基本的主机级安全机制的IPSec、提供IPsec安全机制协商的ISAKMP、 提供对DNS机制保护的DNSsec、提供对MIME格式封装内容保护的Security/Multipart、安全机制中证书标准X.509v3、提供传输层安全机制的TLS以及其他安全机制。

IPSec协议的基本思想是利用认证、加密等方法在IP层为数据传输提供一个安全屏障。与其他层次相比，在IP层实现数据通信安全具有更多的优点。IPSec协议是在IP层实现通讯安全服务最普遍的技术。基于加密技术，IPSec为IPv4和IPv6提供高效的安全服务，包括：存取控制、无连接完整性、数据源认证、数据机密性、抗重传和有限抗流量分析等。

ISAKMP协议属于应用层协议，通过认证将密钥管理、SA的协商双方连接起来，为Internet上的通信提供所需的安全保障。ISAKMP可以为各安全协议层（如TLS，RIPv2等）提供SA协商而不仅仅为IPSec服务。

DNSSec协议主要功能有3项：①提供数据来源验证，验证DNS数据来自正确的域名服务器；②提供数据完整性验证。验证数据在传输过程中没有任何更改；③提供抗否定验证。对否定应答报文提供验证信息。

X.509v3证书标准：数字证书（Certificate）是一段包含用户身份信息、公钥信息以及身份认证机构（CA）数字签名的数据。可信认证中心作为权威的、可信赖的、公正的第三方机构，负责为各种认证需求提供数字证书的签发和管理等服务。

基于协议的安全体系结构描述了信息系统采用的网络协议和安全协议与网络各层的关系。802.10协议为局域网提供了互操作安全规范标准（SILS），属于数据链路层和物理层安全规范。传输层和网络层可以采用符合OSI传输层和网络层的安全协议，也可以采用TCP/IP对应的安全协议如IPSec协议。传输层之上的高层安全协议需要根据具体应用而定。应用层安全协议应根据所采用的网络应用软件而定，由应用软件的安全协议组件提供，不存在通用的应用层安全协议，如：认证服务可采用私钥认证协议Kerberos ， 或 公 钥 认 证 协 议 X.509 ， 安 全 网 络 管 理 服 务 可 采 用SNMPv3协议。

（2）基于实体的安全体系结构

基于实体的信息系统安全体系结构的基本思想：系统功能由各种分配相应的安全功能实体（包括应用实体、服务实体、系统实体及管理实体）完成，为了向系统用户提供安全服务，就需要给各种实体分配相应的安全功能。

每一类实体都将拥有自己的安全结构，与基于协议的安全体系结构不同，它强调实体之间的联系以及实体的安全问题，强调安全管理以安全政策为中心，并把安全管理功能落实到具体实体中。

（3）基于对象的安全体系结构

基于对象的信息系统安全体系结构是针对基于对象技术的分布式信息系统的安全服务规范，其中包括对象管理组（OMG）与1999年修订的CORBA（公共对象请求代理体系结构）安全服务规范，它可以为异构分布式系统提供统一的安全框架。

基于CORBA的安全系统中，安全服务的实现需要一个两层框架：一层建立在CORBA安全服务底层结构上，另一层建立在应用层上。根据实现的功能不同，在实现中将系统划分为4个模块，分别为：应用调用模块、数据库连接模块、数据库操作模块、管理维护模块。

（4）基于代理的安全体系结构

基于代理的信息系统安全体系结构是一种运用软件代理技术实施信息系统安全机制，从而实现安全服务的框架。总的来看，根据不同的应用需要和实现技术，基于代理的安全体系结构具体内容是不同的，但都强调安全策略的动态适应性和主动性。

（5）基于可信计算的安全体系结构

可信计算的核心技术是在现有硬件基础上增加一层可信机制，从而防止终端系统遭受可能的基于软件，甚至硬件的攻击。

可信计算平台是一组强化的硬件部件，其技术具有以下特性：

1.执行保护：软件在隔离的模式下运行，任何其他程序都不能访问它的代码段和数据段；

2.密封存储：数据进行加密存储，只有在和存储环境一致的情况下才能正确解密；

3.输入保护：保护输入设备不会被监视，或输入的数据不会被恶意程序篡改。

4.显示保护：对显存中的数据进行保护，不允许无关程序访问修改。

5.认证机制：可信计算平台技术对当前环境中的硬件采用认证机制。

6.启动保护：操作系统的启动需在认证保护机制内进行。

可信计算可以作为信息系统安全体系结构的基础，并建立以三重防御架构为核心的安全体系结构，最终确保重要信息系统的机密性、完整性。基于可信计算的信息系统安全体系结构是以安全管理中心为核心，终端安全为基础的可信应用环境、可信边界控制以及可信网络传输组成的三重防御体系。

第三章知识点

**1、物理安全概念**

* 什么是物理安全？

物理安全又称实体安全，它是信息系统安全的基础。

定义1：阻止非授权访问设施、设备和资源，以及保护人员和财产免受损害的环境和安全措施。（武汉大学出版社▪《物理安全》）

定义2：为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境、人员、系统等采取适当的安全措施。（《GB21052-2007 信息安全技术•信息系统物理安全技术要求》）

* 物理安全涉及的内容：设备物理安全、环境物理安全和系统物理安全

**2、设备的安全威胁**

* 包含哪几类？被盗/被毁、电磁干扰、电磁泄露、声光泄露
* 防设备被盗与被毁

设备防盗与防毁是利用设备防盗与防毁措施保护系统设备及其部件不被盗

取或毁坏：智能化防盗技术、BIOS机箱防拆卸、机房安装门禁系统、视频监控系统和红外探测系统……

* 抗电磁干扰的方法

（1）屏蔽：电磁屏蔽是利用金属切断电磁波的传播途径，从而消除电场波、磁场波、平面波由一个区域向另一个区域辐射和感应。

（2）滤波：加滤波器，切断电磁干扰沿信号线或电源线传播的路径。滤波的作用主要是使电子设备的内部产生的噪声不向外泄漏，同时防止电子设备外部产生的噪声进入设备。

（3）接地：良好的接地不仅对抑制电磁干扰有显著效果，而且可以保护设备和人身安全。常见的接地有三种：保护接地、系统接地和屏蔽接地。

* 防电磁泄露的方法

（1）使用低辐射设备：低辐射设备即为TEMPEST设备，采取了防辐射措施，消除产生较强电磁波的根源，将设备的电磁泄露抑制到最低限度。

（2）屏蔽：整体屏蔽、部件屏蔽、元器件屏蔽

（3）滤波：加装滤波器，只允许某些频率的信号通过，而阻止其他频率范围的信号，从而起到防止信息泄露的目的。

（4）电磁干扰器：一种能够发射电磁噪声的仪器，通过辐射电磁噪声降低泄露信息的信噪比，从而达到抗电磁干扰的目的。

* 防声光泄露

（1）为防止光泄密事件，建议将设备摆放在远离窗户的地方，如果实在无法避免远离窗户，可以遮蔽室内灯光或用其他光源（例如蜡烛）制造散射效果。

（2）为了防止光缆窃听，可以采用偏振光时域反射技术（POTDR）和迈克尔逊干涉技术。

（3）为了防止声音泄漏信息，可以采用隔声吸声材料，其隔声性能取决于它的质量、坚硬度、阻尼性质等，如果是多层结构，还要考虑多层板的数量、每层的自身性质、与周围环境的连接情况等。

**3、环境安全（包括基本的温湿度要求等）**

A级

电子信息系统运行中断将造成重大的经济损失；电子信息系统运行中断将造成公共场所秩序严重混乱。

A级是最高级别，主要是指涉及国家安全和国计民生的机房设计。其电子信息系统运行中断将造成重大的经济损或公共场所秩序严重混乱，甚至国家安全受到威胁。如：国家气象台、国家级信息中心和计算中心、重要的军事指挥部门、大中城市的机场、广播电台、电视台、应急指挥中心、银行总行等属A极机房。

B级

电子信息系统运行中断将造成较大的经济损失；电子信息系统运行中断将造成公共场所秩序混乱。如：科研院所、高等院校、三级医院、大中城市的气象台的信息中心、疾病预防与控制中心、电力调度中心、交通（铁路、公路、水运）指挥调度中心、国际会议中心、国际体育比赛场馆、省部级以上政府办公楼等属B级机房。

不属于A级或B级的电子信息系统机房为C级。

A级又称为容错型，电子信息系统机房内的场地设施应按容错系统配置，在电子信息系统运行期间，场地设施不应因操作失误、设备故障、外电源中断、维护和检修而导致电子信息系统运行中断。

B级又称为冗余型，电子信息系统机房内的场地设施应按冗余要求配置，在系统运行期间，场地设施在冗余能力范围内，不应因设备故障而导致电子信息系统运行中断。

C级又称为基本型，电子信息系统机房内的场地设施应按基本需求配置，在场地设施正常运行情况下，应保证电子信息系统运行不中断。

温度：当机房环境温度高至60℃，电子信息系统将不能正常工作，同时会加快微机主板、插头、插座、信号线等的腐蚀速度，会引起接触不良、图像质量下降、线圈骨架尺寸改变等现象。温度过低则导致材料变脆、变硬，使得磁性存储器的性能变差，同时漏电流增加。环境温度的过高或过低都会引发硬件性能的下降，从而导致电子信息系统不能正常工作。电子信息系统的最佳环境温度是21±3℃。

湿度：电子信息系统工作的环境湿度宜保持在40% ~ 60%的范围内，过高或过低对系统运行的可靠性和安全性都会产生不良影响。在环境湿度过低的情况下，空气过于干燥，容易产生静电，此时在触碰mos器件时，很容易引起错误的动作，甚至有可能使器件被击穿。在环境相对湿度高于60%时，元器件的表面容易附上一层薄薄的水膜，这水膜不仅会使元器件腐蚀发霉，还会引起元器件各引脚间出现漏电的现象。

灰尘：《174规范》规定A级和B级主机房的含尘浓度，在静态条件下测试，每升空气中大于或等于0.5μm 的尘粒数应少于18000粒。

有人值守的主机房和辅助区，在电子信息设备停机时，在主操作员位置测量的噪声值应小于65dB(A)。

主机房内无线电干扰场强，在频率为0.15~1000MHz 时，主机房和辅助区内的无线电干扰场强不应大于126dB。

主机房和辅助区内磁场干扰环境场强不应大于800A/m。

在电子信息设备停机条件下，主机房地板表面垂直及水平向的振动加速度值不应大于500mm/s2。

主机房和辅助区的绝缘体的静电电位不应大于1KV。

**4、TEMPEST技术**

* 目标

最早的含义是瞬时电磁脉冲发射标准，现在已经演变成了电磁泄漏发射和声光泄漏发射的总称。

研究TEMPEST技术的目的是降低或抑制有用信息的电磁发射。抑制电磁泄漏的方法是电子隐蔽技术（包括用干扰、跳频等技术来掩盖全部电子信息设备的工作状态和保护信息）和物理抑制技术（通过屏蔽或降低功率的方式抑制一切有用信息的外泄，分为包容法、抑源法和Soft-tempest技术）。

* 内容

（1）研究信息处理设备的电磁泄漏机理。分析有用信息是如何加载到辐射信号上的，以及电子信息处理设备的电气特性和物理结构对电磁泄漏的影响。

（2）研究电磁泄漏的防护技术。分析电磁泄漏中，元器件、电路设计和印刷电路板所起的作用，研究各种屏蔽材料、屏蔽结构对电磁的屏蔽效果。

（3）研究有用电磁信息的提取技术。即：电磁信号接收技术和电磁信号还原技术。

（4）研究电磁泄漏测试技术和标准。

（5）TEMPEST材料、元器件和设备的研制。

主要技术措施

（1）屏蔽技术

（2）滤波技术

（3）电磁干扰器

（4）保证安全距离

（5）低辐射技术

不同安全等级的物理安全平台为相对应安全等级的信息系统提供应有的物理安全保护能力。

（1）第一级物理安全平台为第一级用户自主保护级提供基本的物理安全保护。

（2）第二级物理安全平台为第二级系统审计保护级提供适当的物理安全保护。

（3）第三级物理安全平台为第三级安全标记保护级提供较高程度的物理安全保护。

（4）第四级物理安全平台为第四级结构化保护级提供更高程度的物理安全保护。

（5）第五级物理安全平台为第五级访问验证保护级提供最高程度的物理安全保护。

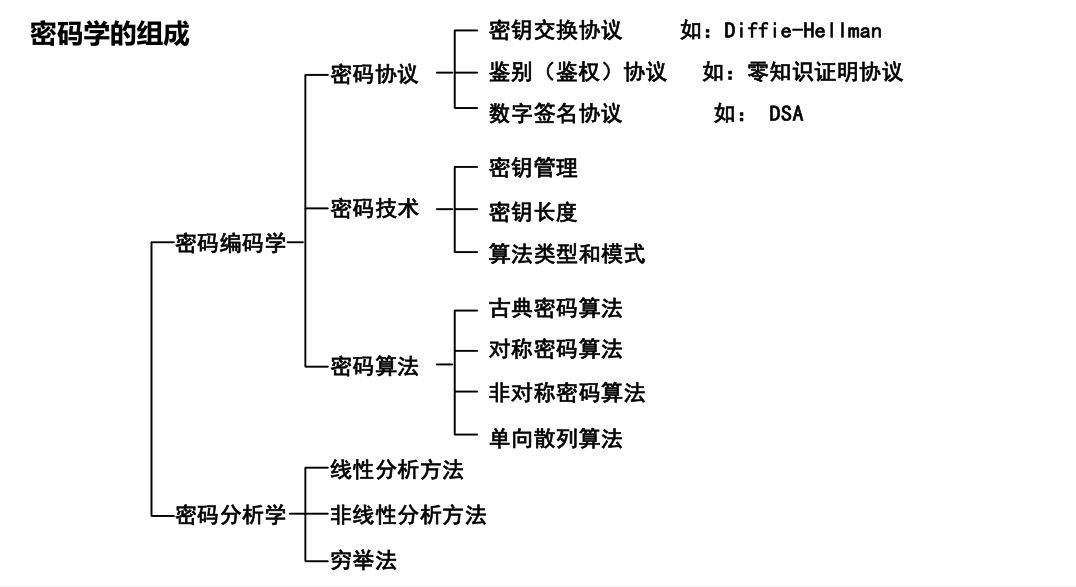
**第四章知识点**

**1、身份认证的方法**

* 基于密码技术、基于生理特征、基于行为特征
* 身份认证：认证对等实体的唯一性

**2、基于公钥密码技术的身份认证**

* 密码编码学的组成



* 公钥密码技术解决了对称密码的哪些困难问题

对称加密算法：通信双方所持有，接收方通过验证发送方是否持有该密钥来验证发送方的身份，一旦出现纠纷，无法进行裁决，这是因为对称密钥无法唯一标识用户的身份。

公钥密码算法：私钥只由用户自己保存，在不泄密的情况下，它可以唯一标识用户的身份，因此，无论是在传输过程中验证用户的身份，还是在后续的仲裁，它都可以作为验证用户身份的依据。

1、在网络环境中，利用传统密码技术无法实现密钥的分配；

2、利用传统密码技术无法数字签名

辨析

Diffie-Hellman算法，主要用于密钥交换，不能用于信息加/解密和数字签名；RSA算法和ECC算法，可以用于密钥交换、加/解密和数字签名；DSA算法只能用于数字签名，不能用于密钥交换和信息加/解密。

误区一：公钥密码比对称密码更安全。

任何密码算法的安全性都是依赖密钥的长度和破解密文所需要的计算量。因此，从密码分析角度，既不能说公钥密码算法比对称密码算法安全，也不能说对称密码算法比公钥密码算法安全。

误区二：公钥密码完全可以替代对称密码。

现有的公钥密码算法所需要的计算量远大于对称密码算法，如果将公钥技术直接用于消息的机密性保护，则系统原有的性能会显著下降。因此公钥密码技术一般用于加密少量的信息，如：密钥交换和数字签名等一类应用。

误区三：与对称密码相比，公钥密码实现密钥分配更加容易。

尽管利用对方的公钥加密共享密钥能够保证密钥交换过程中的机密性，但我们忽略了一个问题：你怎么知道这个公钥就是对方的，而不是假冒的？为此，需要借助某种形式的协议，有时甚至需要一个可信的第三方的参与，通过公证的形式将公钥和用户的身份进行捆绑，而这个过程一点也不比对称密码技术中的密钥分配方法简单。

* 公钥密码技术的基本组成和满足的要求

密钥成对出现，任何一个密钥都可以用来加密，另一个用来解密。

私钥：由用户持有，对其他任何人都是保密的；

公钥：对外公开，任何人都可以通过公开的渠道获取特定用户的公钥。

仅根据密码算法和公钥推导出私钥是不可能的。

公钥密码技术由6部分组成：

1、明文（用M表示）；2、密文（用C表示）；3、私钥（用PR表示）；4、公钥（用PU表示）；5、加密算法（用E表示）；6、解密算法（用D表示）。

针对上述问题，解决的办法是：公私钥只对小数据块加密，即：在认证过程中，需要用一个称为认证符的小数据块替代待加密的文件。

明文和认证符之间必须具有：一一对应关系；明文的任何一点变化都会引起认证符的变换；明文可以计算出认证符，但认证符无法计算出明文。如：散列值具有这些特性。

利用发送方的私钥加密该认证符既可以达到签名的目的，又可以利用很小的存储空间保存加密结果，留待多次认证；针对加密过程，需要产生会话的对称密钥，利用该密钥加密待传输的明文，而接收方的公钥只负责加密会话密钥即可。此时，不仅提高了明文加密的效率，而且对传输开销影响不大。

公钥密码技术满足的要求

（1）用户产生一对密钥（公钥PU和私钥PR）在计算上是容易的。

（2）已知接收方B的公钥和待加密的消息M，发送方A产生相应的密文C，即在计算上是容易的。

（3）接收方B使用其私钥解密收到的密文C，即在计算上是容易的。

（4）已知公钥PU，攻击者解出私钥PR在计算上不可行。

（5）已知公钥PU和密文C，攻击者恢复出明文M在计算上不可行。

（6）加密顺序和解密顺序可以互换，即。

条件1-3：公钥密码算法的工程实用要求，只有算法高效，算法才有实用价值。

条件4-5：公钥密码算法的安全性要求，也是公钥密码算法的安全基础，满足这个条件很难，目前只有RSA和ECC两个算法。

条件6：满足条件的算法多。但同时满足上述条件，需要寻找合适的陷门函数。

* 数字签名有哪些特征？为什么对称密码算法不能用于数字签名？

依赖性：数字签名的内容必须是与消息相关的二进制位串。

唯一性：数字签名必须使用发送方某些特有的信息，以防伪造和否认。

 易用性：产生数字签名比较容易。

 易验证：识别和验证签名比较容易。

 抗伪造：伪造数字签名在计算上不可行。既不能从给定的数字签名中伪造消息，也不能从给定的消息中伪造数字签名。

 可保存：保存数字签名的拷贝是可信的。

对称加密算法无法阻止双方的相互攻击，如：发送方A否认曾经发送过的消息，而接收方B无法证明消息确实来源与发送方A。同时，接收方B也可以伪造发送方A发送的消息，而发送方A无法证明该消息是不是自己发出的。

对称密码算法无法用于数字签名，因为密钥为通信双方所持有，接收方通过验证发送方是否持有该密钥来验证发送方的身份，一旦出现纠纷，无法进行裁决，这是因为对称密钥无法唯一标识用户的身份

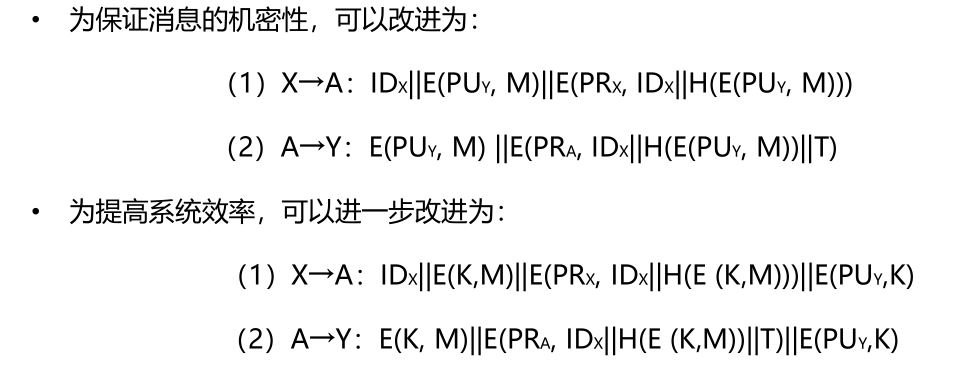
* 直接数字签名和仲裁数字签名

直接数字签名只与通信双方有关，与任何第三方无关。发送方可以使用自己的私钥对整个消息或消息的散列值加密产生数字签名，接收方则通过获得的发送方公钥解密，从而验证签名的有效性。但无论哪种签名方式都无法保证消息的机密性。（因为是私钥加密，任何拥有公钥的接收方都可以查看明文）

解决方法：1、利用对称密钥（或接收方的公钥）加密整个消息和签名结果；2、首先对消息进行加密，然后再对加密的消息签名。

实际应用中，一般选择方案1，但在某些特殊情况下，我们也会采用方案2。直接数字签名也存在一定的安全隐患，即：这种签名的有效性依赖于发送方私钥的安全性。

仲裁数字签名需要第三方仲裁者的介入。仲裁者是关键，它必须是可信第三方。工作原理：发送方X将每条发送给接收方Y的消息首先发送给仲裁者A，A对消息及其签名进行检查，从而验证消息的来源和消息的内容是否被篡改，然后，将该消息加上时间戳后发送给接收方Y，同时告诉Y，该消息已通过仲裁者检验。



此时，仲裁者A既完成了对X发送给Y的消息签名，也保证了消息的机密性，同时兼顾了系统的性能.

**3、认证协议**

* 重放攻击的类型以及防止重放攻击的方法

简单重放：攻击者只是简单地复制消息并在以后重放这条消息。

可检测的重放：攻击者在有效的时限内重放有时间戳的消息。

 不可检测的重放：由于原始消息可能被拦截而无法到达接收方，只有重放的消息到达了接收方，此时就会产生该种攻击。

 不可修改的逆向重放：这是针对消息发送方的重放。如果使用对称密码，而且发送方无法根据内容区分出是发送的消息还是接收的消息，则会产生该种攻击。

对付重放攻击的方法主要有以下几种：

（1）序列号：在每个用于认证的消息后附加一个序列号，只有序列号正确的消息才能被接收。但是这种方法存在一个问题，即它要求参与通信的每一方都必须记住其他通信各方最后附加的序列号。如果身份认证是一个不确定的过程，则通信一方要记住所有可能通信参与方的最后序列号，这是不可行的，特别是对于资源受限的实体更是如此，因此在身份认证过程中，一般不使用序列号。

（2）时间戳：在每个用于认证的消息后附加一个时间戳，接收方在看到这个时间戳后，与其所认为的当前时间进行比对，当两个时间足够接近时，接收方才认为收到的消息是新消息，否则丢弃。但这种方法要求通信各方的时钟保持同步，一旦通信一方的时钟机制出错而使同步失效，则攻击成功的可能性将会增大；同时，在有些环境中实现时钟是很困难的，如：网络延时不可预知的网络环境。

（3）挑战/应答：若 A 要接收 B 发来的消息，则 A 首先要给 B 发送一个临时交互号（挑战码），并要求 B 发来的消息（应答）中包含该临时交互号。但这种方法不适合面向无连接的应用，如：邮件系统。因为它要求在任何无连接传输之前必须先握手，这与无连接信息交互的特征相违背。

* 双向认证协议和单向认证协议

双向认证协议又称为相互认证协议，可以使通信双方在确认对方身份的基础上交换会话密钥。在这个过程中，保密性和及时性是身份认证中的两个重要问题。

身份认证分为单向认证和双向认证，如果通信过程中只需要一方验证另一方的身份，则这样的认证过程为单向认证，如电子邮件系统；如果通信过程中需要相互认证通信参与方的身份，则这样的认证过程为双向认证，如登录电子银行处理相关业务。对于直接数字签名和仲裁数字签名的过程，可以认为是单向认证协议，即：接收方通过验证发送方或仲裁者的签名结果，来验证发送者的身份。

**4、基于生理特征的身份认证**

基于人体固有的生理特征进行身份认证，需要利用传感器采集生理特征信息，并利用计算机进行处理。生理特征必须具有：

普遍性，即每个人都必须具有的特征；

唯一性，即不同的人，其特征必定不同；

可测量性，即这个特征是可以采集，计算机可处理；

稳定性，即特征不会随时间改变而改变；

安全性，即不容易被伪造或模仿。

如：指纹识别技术、虹膜识别技术、人脸识别技术、DNA识别、声纹识别、手形识别、掌纹识别和人耳识别等。

**5、基于行为特征的身份认证**

步态识别技术、笔迹识别技术

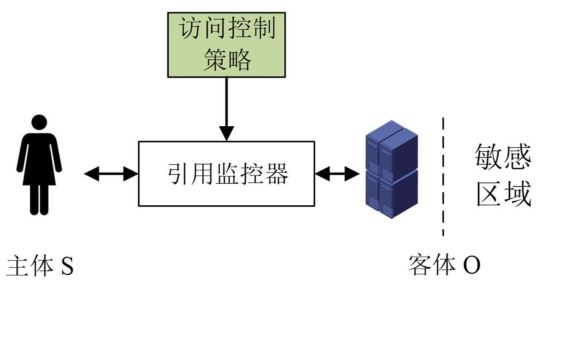
**第五章知识点**

**1、访问控制概述**

* 什么是访问控制？访问控制模型及其四个要素

访问控制是对主体访问客体的能力或权力的限制，根据用户的权限不同，用户被授予了不同资源的访问能力，而未授权的用户无权访问该资源，这是由信息系统的访问控制技术来保证的。

目的：限制用户访问信息系统的能力，是在保障授权用户获取所需资源的同时，阻止未授权用户的安全机制，同时保证敏感信息不被交叉感染。



它包括四个要素：

（1）主体S：是提出访问资源请求或某一操作动作的主动发起者，但不一定是动作的执行者。它可以是用户、计算机进程、服务和设备等，它产生信息的流动和系统状态的改变。

（2）客体O：是被访问资源的对象，在信息流动中处于被动地位。客体可以是被操作的信息、资源，也可以是网络上的硬件设备或终端。甚至一个客体可以包含另一个客体。

（3）引用监控器：它是监督主体和客体之间授权访问关系的部件，实现时

采用引用验证机制，引用验证机制必须同时满足以下三个原则：具有自我保护能力；总是处于活跃状态；必须设计的足够小。

（4）访问控制策略：是主体对客体的相关访问规则集合，即属性集合。既定义了主体对客体的动作或行为，也给出了客体对主体的条件约束，遵循的原则：最小特权原则（最大限度地限制了主体行为，可避免来自突发事件、操作错误）和未授权主体等意外情况的危险）；最小泄露原则；多级安全原则。

* 引用控制器遵循的三个原则？具有自我保护能力、总是处于活跃状态、必须设计的足够小
* 访问控制策略遵循的三个原则？最小特权原则、最小泄露原则、多级安全原则
* 访问控制的描述方法及其特点。访问控制矩阵、访问控制列表、访问能力表、授权关系表

访问控制可以用一个二元组（控制对象，访问类型）来描述，其中控制对象是指信息系统中一切需要进行访问控制的资源，访问类型是指对于相应的受控资源的访问操作，如读、写、创建、修改和删除等。

（1）访问控制矩阵

访问控制矩阵又称为访问许可矩阵，用二维矩阵描述了任意主体和任意客体的访问权限。其中Own表示所在行的主体对所在列的客体拥有管理权限，能够授予或撤销其他用户对该客体的访问权限，R表示读操作，W表示写操作，E表示删除操作。

访问控制矩阵的实现易于理解，清楚描述了主体对客体的访问权限，但是查找和实现起来有一定的难度，而且，如果信息系统比较庞大，用户和文件系统要管理的文件很多，那么控制矩阵将会成几何级数增长，这样对于增长的矩阵而言，会有大量的剩余空间，造成很大的存储空间的浪费。

（2）访问控制列表

访问控制列表（ACL）是从客体（列）出发，表达访问控制矩阵某一列的信息，用来对某一特定资源指定任意一个用户的访问权限。它是将访问控制矩阵按列存储，每个客体均有一个主体明细表，表示对该客体具有访问权限的主体及其相应的访问模式。

使用ACL进行访问权限管理时，不仅可以依靠单个用户进行权限管理，而且可以将用户按组进行组织，用户可以从用户组取得访问权限。尽管ACL表述直观，易于理解，比较容易查出对某一特定资源拥有访问权限的所有用户，有效地实施授权管理。但对于较大规模的信息系统而言，系统资源很多，ACL需要设定大量的表项，而且修改起来比较困难，实现整个组织范围内一致的控制策略也比较困难。而且单纯使用ACL，不易实现最小权限原则及复杂的安全政策。

（3）访问能力表

与访问控制列表正好相反，是从主体（行）出发，表示某一主体对不同客体的访问权限，它决定了主体是否能够访问客体，以及用什么方式访问客体。

主题可以将能力转移给为自己的工作的进程，而且在进程运行期间，主体可以动态地下发、回收、添加或删除某种能力。这种能力的转移不受任何策略的限制，这种方式给用户带来灵活性的同时，也带来了安全隐患。如果接受能力转移的进程已经被感染或是恶意程序，那么，客体的信息就会泄漏。如果客体是信息系统的关键资源，则必然会给信息系统带来灾难性的后果。

通过查询访问能力表，很容易获得一个主体授权访问的所有客体及其权限，但从客体出发获得哪些主体可以访问它就比较困难。

（4）授权关系表

描述了主体和客体之间各种授权关系的组合。如果这张表按客体进行排序，授权关系表将得到与访问控制列表相当的二维表；如果这张表按主体进行排序，授权关系表将得到与访问能力表相当的二维表。

* 访问控制实现的类别？接入访问控制（用户首先需要与信息系统进行远程连接，只有通过认证的用户才能访问系统）、资源访问控（然后在权限控制下，访问其对应的资源）、网络端口和节点的访问控制（最后，获取的资源需要通过网络中的不同节点和端口才能返回用户，防止被篡改或监听）。
* 资源访问控制涉及哪些内容？文件系统的访问控制（文件目录访问控制和系统访问控制）、文件属性访问控制、信息内容访问控制

**2、基于所有权的访问控制**

* 自主访问控制和强制访问控制的概念？

自主访问控制DAC：自主访问控制是指资源的所有者不仅拥有该资源的全部访问权限，而且能够自主的将访问权限授予其他的主体，或从授予权限的主体收回其访问权限。

强制访问控制MAC：不再让普通用户管理资源的授权，即使是资源的创建者也不行，而将资源的授权权限全部收归系统，由系统对所有资源进行统一的强制性控制，按照事先制定的规则决定主体对资源的访问权限。

* 自主访问控制策略的分类和重要标准
  + 分类：严格的自主访问控制策略（不可代理）、自由的自主访问控制策略（可代理）和属主权可以转让的自由访问控制策略（权力可转让）
  + 重要标准：文件和数据等资源的所有权、访问权限及批准
* 强制访问控制的保密性规则和完整性规则

保密性规则：

仅当主体的密级高于或者等于客体的密级时，该主体才能读取相应的客体（下读）；仅当主体的密级低于或者等于客体密级时，该主体才能写相应的客体（上写）。

完整性规则：

仅当主体的完整性级别低于或者等于客体的完整性级别时，该主体才能读取相应的客体（上读）；仅当主体的完整性级别高于或者等于客体的完整性级别时，该主体才能写相应的客体（下写）。

* BLP模型的访问规则及其举例？简单安全性访问规则、\*安全性访问规则、自主安全访问规则

保护数据的机密性，但无法阻止未授权主体修改客体信息，破坏其完整性。其基本安全策略是“下读上写”，即主体对客体向下读、向上写，保证敏感信息不泄漏。

隐蔽通道是指不在安全策略控制范围内的通信通道。由于BLP模型允许低密级的主体向高密级的客体写入，即“上写”，这将带来潜在的隐藏通道问题。

* BiBa模型的访问规则？

保护数据的完整性，Biba模型规定，信息只能从高完整性等级向低完整性等级流动，为此，它将完整性等级从高到低分为三级：关键级（C），非常重要（VI），和重要（I），它们的关系为C＞VI＞I。

访问方式：修改（modify）、调用（invoke）、观察（observe）、执行（execute）。

* + 非自主安全访问规则及特点？严格完整性规则，针对主体的下限标记规则，针对客体的下限标记规则，下限标记完整性审计规则，环规则。

Biba模型的优点：Biba模型和BLP模型相对独立。前者是完整性访问，后者是保密性访问；模型简单；可以与BLP模型结合。

Biba模型的缺陷：Biba模型的目的性不明确；完整性级别的标签确定困难；Biba模型与BLP模型结合困难。

* 自主安全访问规则？访问控制表、客体层次结构和环（环用数字表示，数字越低，权限越高）

**3、基于角色的访问控制**

* 基本概念

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。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限，但用户不直接与权限关联。

好处：不必在每次创建用户时都进行分配权限的操作，只要分配用户相应的角色即可，而且角色的权限变更比用户的权限变更要少得多，这样将简化用户的权限管理，减少系统的开销。

* 角色继承、角色限制、角色的分配与授权

角色：角色是指一个可以完成一定事务的命名组，它代表了一种权利、资格和责任，不同的角色通过不同的事务来执行各自的功能。

事务：事务是指一个完成一定功能的过程，可以是一个程序或程序的一部分。

角色继承：反应系统内部角色之间的权利、责任关系。可以用“父子”关系表示。

角色的分配与授权：一个角色授权给一个用户是指该角色分配给这个用户。

角色限制：角色限制包括角色互斥和角色基数限制，而角色互斥分为静态互斥（分配阶段）和动态互斥两种（会话选择阶段）方式。

会话：用户是一个静态的概念，会话是一个动态的概念，用户通过建立会话激活角色，从而对资源进行访问。

* RBAC模型

RBAC模型族中从简单到复杂一共有4个模型：RBAC0、RBAC1、RBAC2和RBAC3。RBAC0是基本模型，它包含了支持RBAC的最低要求；RBAC1增加了角色层次的概念，（数字小等级高）又称为角色分级模型；RBAC2增加了约束，又称为限制模型；而RBAC3把RBAC1和RBAC2组合在一起，提供角色分级和继承的能力，又称为统一模型。

RBAC0包含三个实体集（用户集、角色集、权限集）和会话；RBAC1增加了角色等级；RBAC2增加了约束的概念；RBAC3包含RBAC1中角色等级的概念和RBAC2中的约束规则。

角色限制原则：用户所拥有的权限不得高于他在执行指定操作时所需要的权限，即最小权限规则。

职责分离：对于一个敏感任务，可以分配两个职责上互相约束的两个角色来实现。

互斥角色：是指同一个用户只能分配一个互斥角色集合中至多一个角色，或者某一个用户即使分配了一个互斥集合中两个或两个以上的角色，但在应用中只能使用其中一个。

角色容量：在特定的时间段，某些角色不能超过固定数量的用户。

先决条件角色：有些角色，在获得之前必须具有一定的条件。

时间频度限制：规定了角色允许使用的时间和特定角色允许使用的频度。

**4、基于任务的访问控制（TBAC）**

* 特点？任务是否有权执行受任务顺序限制和任务的依赖关系限制，依据任务之间的相互关系来决定使用者拥有的权限

基于任务的访问控制（TBAC）采用“面向任务”的观点，从任务（活动）角度建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。在TBAC中，对象的访问权限控制不是静止不变的，而是随着执行任务的上下文环境发生变化，它是一种主动访问控制模型。

三层含义：

（1）TBAC是在工作流的环境中考虑对信息的保护问题。上下文相关的访问控制模型。

（2）TBAC不仅能对不同工作流实行不同的访问控制策略，而且还能对同一工作流的不同任务实例实行不同的访问控制策略。

（3）任务都有时效性，所以在TBAC中，用户对于授予他的权限的使用也是有时效性的.

* 授权步、任务、授权单元和依赖

授权步：表示一个原始授权处理步（在一个工作流中对处理对象的一次处理过程）。

任务：任务是工作流中的一个逻辑单元，完成某种特定的功能。

授权单元：授权单元是由一个或多个授权步组成的结构体。

依赖：依赖是授权步之间或授权单元之间的相互关系。

* TBAC模型

在工作流环境中，对数据的处理与上一次的处理结果相关联，相应的访问

控制也是如此。

在TBAC中，某个任务是否有权执行，要看此任务与其他相关任务之间维

持着怎样的关系。任务之间的关系包括：

任务顺序限制：在企业内部的任务，有些是可以被并行处理，有些任务必须依次执行

任务的依赖限制：两个任务具有执行的相关性。

（1）TBAC的特点是在任务执行时，依据任务之间的相互关系来决定使用者拥有的权限。

（2）TBAC着重于任务流程和任务生命周期的管理。

（3）TBAC模型一般用五元组（S，O，P，L，AS）来表示，其中S表示主体，O表示客体，P表示许可，L表示生命期（lifecycle），AS表示授权步。

（4）TBAC中，访问控制策略包含在AS-AS，AS-U，AS-P的关系中。

（5）TBAC从工作流中的任务角度建模，可以依据任务和任务状态的不同，对权限进行动态管理。

**5、基于属性的访问控制**

* 属性类别？主体属性、客体属性、环境属性和权限属性

基于属性的访问控制（ABAC）是通过对实体属性添加约束策略的方式实现主客体之间的授权访问。在ABAC模型中，并不关心访问者是谁，而只需知道访问者具有哪些属性，这就使得一个访问控制系统中的2个不同实体，在另一个访问控制系统中可能映射为具有相同属性的2个主体。

主体属性：主体属性通常与其身份和特征密切相关。

客体属性：客体的属性通常有客体属主、客体类型、客体容量和客体安全级别等。

环境属性：环境属性是指访问操作进行前或者访问操作进行时的一些环境信息。

权限属性：操作的权限是对资源的打开、读、写、修改和删除等一系列操作。

* 授权思想和模型？

授权思想：根据信息系统预先定义的安全策略，对提出访问请求的主体，依据其拥有的属性特征集、客体特征属性集和相应的环境属性特征集进行授权决策。

步骤1：策略执行点（PEP）接收原始访问请求（NAR）。

步骤2：根据NAR，利用不同的属性权威（AA）中存储的信息构建一个基于属性的访问请求（AAR）。AAR描述了请求者、资源、方法和环境属性。

步骤3： PEP将AAR传递给策略判定点（PDP）。

步骤4： PDP根据从策略管理点（PAP）处获取的策略对AAR进行判定，并将判定结果传给PEP。

步骤5： PEP执行此访问判定结果。

**第六章知识点**

**1、操作系统安全概述**

* 面临的安全威胁？

病毒：能够自我复制的计算机程序，破坏计算机功能，具有隐蔽性、潜伏性、破坏性、寄生性、传染性。

蠕虫：具有传染性和复制功能，但与病毒不同，蠕虫是一个单独的程序，可以独立存在，无需寄生在某个程序之中。

木马：表面上在执行合法的功能，实际上能在不破坏系统的任何安全规则的情况下进行非法活动。木马与一般的病毒不同，它不会自我复制，也不“刻意”地去感染其他文件，它通过伪装自身，吸引用户下载执行，向实施者打开被感染主机的门户，使实施者可以任意毁坏、窃取被感染主机的文件，甚至远程操控被感染的主机。

逻辑炸弹：是指在特定逻辑条件满足时，实施破坏的计算机程序，该程序触发后造成计算机数据丢失、系统瘫痪等。

隐蔽通道：是指系统中不受安全策略控制的、违反安全策略的信息泄露路径。分：隐蔽存储通道和隐蔽定时通道。

天窗（后门）：又称后门，是嵌在操作系统里的一段非法代码，它能绕过系统安全策略控制而获取对程序或系统访问权。

操作系统安全是信息系统安全的基石。操作系统的安全性是必需的。安全操作系统的安全性则是特色。安全操作系统是针对安全性开发增强的，并且与相应的安全等级对应。

* 操作系统的硬件安全机制？存储保护、运行保护和I/O保护

存储保护是指保护用户在存储器中的数据，它是操作系统安全最基本的要求。存储保护的精度取决于保护单元的大小，保护单元越小，存储保护的精度越高。同时提高存储空间的利用率。但因为存储单元小，会造成文件存储时分散到不同的存储区域，从而占用较多的页面，导致文件或进程的页表长，占用较多的内存，同时，还会降低页面换进换出的效率。如果存储单元比较大，可以减少页表的长度，提高页面换进换出的速度，但存储保护的精度低，而且会造成存储的碎片太多，造成存储空间的浪费。

若内存中一次只能运行一个进程的操作系统，存储保护机制应能够防止用户程序对操作系统的影响。若内存中可以一次运行多个进程的多任务操作系统，则还需要进一步要求存储保护机制对各进程的存储空间进行隔离。存储保护与存储管理密切联系的。存储保护机制保证系统中各进程之间互不干扰，而存储管理则是为了更有效地利用存储空间。

运行保护是隔离操作系统程序与用户程序，免受同等级运行域内其他进程的破坏。运行域是一种基于保护环的等级域结构，它是进程运行的区域，环号越小，权限越高。等级域机制是用于保护某一环不被其外层环侵入，并且允许在某一环内的进程能够有效地控制和利用该环以及抵御该环特权。进程隔离与等级域机制的区别：一个进程，它可以在任意时刻在任何一个环内运行；在运行期间还可以从一个环移动到另一个环；系统将隔离在同一环内同时运行的各个进程。

* 什么是最小特权管理

所谓特权是指可违反系统安全策略的一种操作能力，它与访问控制相结合，提供系统的灵活性。

好处：1、执行一些受限的操作或进行违反安全控制策略的操作，一般用户不可以；2、可以执行任意操作，便于系统的维护和配置。

风险：1、一旦超级用户的口令丢失或超级用户被冒充，将会对系统造成极大的损失。2、超级用户的误操作。

最小特权管理的思想是系统不应给用户超过执行任务所需特权以外的权限，或仅给用户赋予必不可少的特权。一方面赋予主体“必不可少”的特权；另一方面它仅给用户“必不可少”的特权。

 不应对某个用户赋予一个以上的职责，应将超级用户的特权划分为一组细粒度的特权：

系统安全管理员：拥有安全管理特权集，是整个系统安全策略的制定者；

审计管理员：拥有审计管理特权集，是系统的监督者；

系统管理员：拥有系统管理特权集，管理与系统相关的资源。

**2、Windows操作系统安全**

* 安全机制包含哪些？其工作原理是什么？用户账号管理、身份认证、访问控制、安全审计和文件加密

用户账号管理机制：至少有两种类型的账号，即系统管理员账号（操作系统安装时，自动分配。属于超级用户，拥有操作系统的所有权限）和普通用户账号（拥有部分权限，由管理员分配）。

身份认证机制：身份认证除了用户登录操作系统验证身份外，还需要验证对象和服务的身份。按照登录的方式不同，Windows操作系统提供了两种基本的身份认证类型（本地认证和网络登录）。

访问控制机制：Windows7操作系统的安全性达到了TCSEC（橘皮书）标准的C2级，通过对用户授权来决定用户可以访问哪些资源，以及对这些资源的访问能力。其访问策略包括：自主访问控制、强制访问控制、基于角色的访问控制。

在Windows7中，当用户希望共享某个自己创建的对象时，它不能为其他用户和组分配权限，权限的分配必须通过系统管理员来完成。在Windows系统中，访问控制列表可以分为自主访问控制列表和系统访问控制列表两类。

自主访问控制列表(DACL)由对象的所有者控制，每个表由表头和零个或多个ACE组成，ACE决定了用户或组执行该对象的类型。系统访问控制列表(SACL)实际上是一个审计中心，该列表描述了该对象上的哪些类型的访问请求需要被系统记录。

安全审计机制：为了跟踪用户的各项操作，系统需要对安全事件进行审计，并写入安全日志中。在Windows7中，审计策略配置分为：

基本审计策略配置：除登录事件外，所有的审计内容默认都是关闭的，必须通过手动的方式打开审计进程来审计目标对象，并指定审计失败还是成功的事件。

高级审计策略配置：允许管理员选择要监视的行为，也可以排除审核结果以供您选择。

事件的审计类型可以分为两类：成功事件和失败事件。（1）记录失败事件不仅可以查看哪些操作失败了，从而可以分析失败的原因；（2）记录成功事件，是因为攻击者通过非法的手段获得访问权限后，也会生成一个成功事件，通过该事件我们可以对攻击事件溯源。

文件加密机制：Windows的文件加密机制与系统安全控制逻辑的结合。在一定的不可靠环境中，存储和处理用户信息时，保持其私密性、不可篡改的完整性等安全属性。Windows加密机制分为两个部分：

 第一部分是基本的加密算法服务。摘要、对称加密和非对称加密等基本的加密算法可以通过下一代CryptoAPI（CNG）的API接口，被应用程序调用。

 第二部分是Windows系统加密功能。内容包括加密文件系统（EFS）、用户信息保护和SSL等网络加密协议等。它一方面保护Windows系统（单机和域）的安全，另一方面，也提供了可供应用程序直接使用的系统级加密保护服务。

* 访问控制机制中的安全访问令牌和安全描述符？

Windows7的访问控制机制除了访问控制列表外，还包括以下的安全实体：安全访问令牌和安全描述符。

安全访问令牌：安全访问令牌是LSA模块收到登录用户的SID信息后创建的，它相当于用户访问系统资源的票据。令牌有两类：主令牌和模拟令牌。与安全访问令牌可关联的实体：进程、线程、用户。

安全描述符：安全描述符是与每个被访问对象相关联，描述一个被访问对象的安全信息，其主要组件是访问控制列表，它为访问对象确定了个用户和组的访问权限。

安全描述符的内容如下：

标记：一个控制位集合，说明安全描述符的含义或它每个成员。

用户SID：与安全描述符关联的安全对象的所有者SID。

组SID：与用户SID对应的所有者所在组的SID。

自主访问控制列表（DACL）：确定哪些用户和组对该对象的访问权限。

系统访问控制列表（SACL）：确定该对象上的哪些操作可以产生审计信息。

**3、Linux操作系统安全**

* 文件安全、用户和组安全、进程安全和日志管理安全

目前Linux的安全级已经达到TCSEC评估标准的C2级。

用户和组安全：与Windows系统类似，用户和组是Linux操作系统中进行操作、文件管理和资源使用的主体，它们在操作系统中以不同的角色存在。

文件系统安全：Linux系统能够支持5种基本的文件类型：普通文件、目录文件、设备文件、链接文件和管道文件。

块设备文件：以字符块为单位进行存取；字符设备文件：以单个字符为单位进行存取。链接文件是一种特殊的文件，它是一个真实存在的文件链接，类似Windows下的快捷方式。根据链接文件不同，分为：硬链接文件和符号链接文件。

文件访问权限由10位字符组成，第1个字符指定了文件的类型，横线表示是一个非目录的文件；d表示是一个目录。后面的9个字符，每3个一组，依次表示文件所有者、同组用户、其他用户分别对该文件的访问权限。（只读、只写、可执行）

Linux也通过加密文件系统EFS保护用户的数据。Linux系统中可以使用的加密文件系统有：CFS、TCFS、AFS、eCryptFS、ReiserFS等。eCryptFS是一种堆栈式文件系统，它是利用堆栈的原理开发的一种具有良好可扩展性的文件系统。

进程安全：Linux是一个多用户、多任务的操作系统，它对计算机资源（如：文件、内存、CPU等）的分配和管理都是以进程为单位。Linux跟踪所有进程的活动、进程对系统资源的使用情况，目的是管理进程和资源，协调多个进程对这些共享资源的访问。Linux系统中的进程可以分为3类：交互进程、批处理进程和守护进程。每个进程有三种基本状态：运行态（R），就绪态（W），封锁态（S）（或挂起态）。

启动一个进程有两种途径：手工启动和调度启动。启动方式：前台启动和后台启动。

日志管理安全：Linux系统的日志子系统记录系统每天发生的各类事情。 一旦系统受到攻击后，日志可以记录攻击者留下的痕迹。日志的主要功能是审计和监测，存储在/var/log目录中。Linux日志都是以明文的形式存储，既可以搜索和阅读它们，还可以利用脚本扫描这些日志，并基于它们的内容去自动执行某些功能。Linux系统中有4类主要的日志：连接时间日志、进程统计日志、错误日志、程序日志。

* 用户和组安全涉及内容？安全使用用户和组文件、验证用户和组文件、用户密码的设定方法

安全使用用户和组文件：Linux操作系统的全部用户信息都保存为普通的文本文件，管理员可以通过修改这些文件来管理用户和组。

验证用户和组文件：Linux操作系统提供了pwck和grpck两个命令分别验证用户和组文件，以保证两个文件的一致性和正确性。

用户密码的设定方法：如果密码设置不恰当，就容易被攻击者破解。十二条设置密码口令的原则。

用户账号文件——/etc/passwd：是用户管理文件中的关键文件之一，该文件用于用户登录时效验用户的登录名、加密的口令数据项、用户ID、默认的用户分组ID、用户信息、用户登录子目录以及登录后使用的Shell。

用户影子文件——/etc/shadow：Linux采用“shadow文件”机制，将加密口令转移到shadow文件中，只有root超级用户可读。而在passwd文件中，口令字段处只存放一个“x”或“\*”，从而减少了密文被泄露的机会。（存放系统的用户加密口令）。

组账号文件——/etc/group：passwd文件中包含每个用户默认的分组ID（GID），这个GID在group文件中被映射到该用户分组的名称以及同一分组的其他成员中。

/etc/skel启动文件的目录：/etc/skel目录中一般存放的是用户启动文件的目录，该目录由超级用户root控制。当添加用户时，这个目录中的文件自动复制并添加到新用户的登录子目录下。里面都是隐藏文件，类似.file格式的文件。

/etc/login.defs配置文件：/etc/login.defs文件是创建用户时的一些规则，如：是否需要登录子目录，UID和GID的范围，用户的期限等。该文件只能通过超级用户root来定义。

/etc/default/useradd文件：该文件主要是规定用户登录子目录存放的位置、环境配置文件目录存放的位置以及登录执行的首个Shell等。主要包括如下信 息：用户组ID（GROUP）、用户登录子目录存储位置（HOME）、是否启用账号过期停权标志（-1表示不启用）、账号终止日期（不设置表示不启用）、所有Shell类型所在目录（SHELL）、默认添加用户时需要复制的启动文件位置（SKEL）、为用户建立的邮箱（CREAT\_MAIL\_SPOOL）等。

pwck 用来验证用户账号文件（/etc/passwd）和影子文件（/etc/shadow）的一致性，验证文件的每一个数据项中每个字段的格式及其数据的正确性（致命错误：正确的域数目、唯一的用户名）。

grpck命令是用来验证组账号文件（/ect/group）和影子文件（/etc/gshadow）的一致性和正确性。验证文件的每一个数据项中每个字段的格式及其数据的正确性（致命错误：正确的域数目、唯一的组群标识）。

密码设置：MD5（至少有15个字符）、DES（使用最长长度8个字符）

* SELinux的目标策略

SELinux控制root权限，对root账号采用强制访问控制机制，同时限制用户程序和系统服务器完成任务的最低权限。

 安全上下文：它依附于每个对象（程序、文件、进程等）上，记载着整个对象所拥有的权限。 对象能否执行某项操作受安全上下文和DAC控制。

 类型强制（Type Enforcement，简称TE）规则：它是将权限与程序的访问结

合在一起，而不是结合用户，即进程对文件、目录和套接字等的访问权。规则

制定基于：程序的功能和安全属性；用户要完成任务需要的所有访问权。

 目的：限制到功能合适、权限最小化的程度。

安全上下文核心元素：SELinux用户、SELinux角色、SELinux类型、SELinux类型强制、SELinux级别。

目标策略：Strict示例策略更趋向于最大化使用SELinux所有特性，为大部分程序提供强壮的安全保护，而Targeted策略的目标是隔离高风险程序。

Targeted策略的好处是一方面可以向Linux系统添加大量的安全保护，同时又尽量少地影响现有的用户程序。

相同点：Targeted策略是从Strict示例策略衍生而来的，它们的结构和组织几乎完全一样；

不同点：（1）Targeted策略使用了无限制的域类型unconfined\_t，并移除了所有其他用户域类型，如：sysadm\_t和user\_t等，只有system\_r角色；（2）几乎所有的用户运行的程序都是以unconfined\_t域类型执行，不能分配可写和可执行的内存，降低了缓冲溢出攻击的风险。

使用SELinux模式可以被设置为enforcing（主要模式），permissive（审核遭受拒绝的消息）或disabled（内核机制完全关闭）等3种，它由init使用，在它载入初始策略前配置SELinux使用。

布尔变量通常用来在运行时改变SELinux的部分策略，而不需要重新定义和改写策略文件。setsebool指令：布尔变量的状态改变只是暂时的，一旦系统重启后，该变量恢复初始状态。setsebool –P指令：永久改变状态。

**4、Android操作系统安全**

* Android的安全模型

1、应用程序沙盒

Android继承和扩展了Linux 内核安全模型的用户与权限机制。每个应用程序安装阶段，赋予一个独立的UID。应用执行时，就在特定进程内以该UID运行。无论该进程在什么地方执行，每个应用都有一个只有它才有读写权限的专用数据目录，由此建立了内核级的应用沙盒。因此，Android系统中内存的损坏只影响其对应的程序，其他程序不受影响。

2、访问权限

应用沙盒隔离，只能访问自己的文件和可全局访问的资源。访问的 permission权限。为了扩充其应用，Android通过AndroidManifest.xml文件可以赋予应用额外的、细粒度的权限，从而控制硬件设备、网络连接、数据或系统服务的访问。在应用程序安装时，Android检查请求权限列表，决定是否给予授权。授予的权限不可撤销。权限检查可以在不同层次上执行。

3、IPC-进程间通信

4、SElinux：安卓沿用了Linux安全增强技术SELinux。

* 进程间通信方法

进程隔离：与Linux类似，Android进程的地址空间是独立的，一个进程不能直接访问另一个进程的内存空间。

 Binder机制：即Android使用内核驱动和用户空间层的组合来实现IPC机制。进程通信通过ioctl()调用实现的，它使用binder\_write\_read结构收发数据，该户数据结构由一个read\_buffer和一个write\_buffer组成，其中write\_buffer包含驱动所要执行的命令，而read\_buffer包含用户层需要执行的命令。

 作用：Android系统利用IPC机制帮助进程发现为其提供的服务并与之交互的进程。

 Binder架构：与Windows的COM和Linux的CORBA类似，Android系统也采

用一个基于抽象接口的分布式组件架构，防止提权现象的发生。

* 权限保护级别

normal级是Android系统默认的安全级别，它定义了访问系统或其他应用程序的低风险权限。

dangerous级的权限可以访问用户数据或在某种形式上的控制设备。因此，在赋予权限时，需要用户确认。

signature级是最严格的权限级别，需要持有加密密钥。该权限只赋予那些与声明权限使用相同签名密钥的应用程序。它通常被赋予用于执行设备管理任务的系统应用。

signatureOrSystem级某种形式上是一个折中方案，可被赋予系统镜像的部分应用，或与声明权限具有相同签名密钥的应用程序。允许厂商无需共享签名密钥的情况下，预装自己的应用来共享一个需要权限的特定功能。

* 资源回收机制的原则

当Android系统发现内存不够使用，需要回收时，Android系统的Memory Killer就会杀死其他进程，来回收足够的内存。

 回收原则：Android系统优先清理那些已经不再使用的进程或优先级较低的进程，或是倾向于杀死一个能回收更多内存的进程。

**第七章知识点**

**1、数据库系统安全概述**

* 概念

数据库系统是指一个实际可运行的数据处理系统，它是一个存储、维护和为应用程序提供数据的软件系统，是存储介质、处理对象和管理系统的集合体。

数据库系统一般分为两个部分：数据库和数据库管理系统（DBMS）。

数据库的结构分为：内模式（或内层）、概念模式（或概念层）、外模式（或外层）。

数据库系统安全：数据库安全是保证数据库信息的机密性、完整性、可用性、可控性和隐私性，防止系统软件及其数据遭到破坏、更改和泄漏。

* 数据库系统安全涉及的内容？

涉及的内容：用户身份认证、事务处理访问检查、授权规则、语义完整性检查、用户登录鉴别、审计追踪、操作系统检查、文件检查、实体保护、数据库并发控制、数据库恢复、统计数据安全与推理控制等。

* 操作系统为数据库系统安全提供了哪些辅助功能？

DBMS的安全性依赖于操作系统，因此为了保证DBMS的安全性，操作系统至少提供以下几点安全功能：

（1）保护DBMS，防止用户程序对其修改，尤其是DBMS中的访问控制机制；

（2）对内存缓冲区中的数据提供保护，当敏感数据存放在内存缓冲区中时，必须防止非授权用户对其读写；

（3）防止DBMS之外的程序对数据库直接进行访问；

（4）保证正确的物理I/O，确保读取数据库文件的正确；

（5）提供可靠的数据通信信道，通过通信信道传输数据时，应对其提供保护，防止数据泄漏或被篡改。

* 数据库系统面临哪些安全威胁？

（1）软威胁：病毒、蠕虫和木马；天窗或后门；隐蔽通道；逻辑炸弹。

（2）硬威胁：存储介质故障、控制器故障、电源故障、芯片主板故障。

（3）人为错误：操作人员或系统用户的错误输入或不正确使用应用程式。

（4）传输威胁：数据在传输过程中有可能被监听、否认；信息被重放等威胁。

（5）物理环境威胁：由于地震、火灾、水灾等自然或意外事故造成硬件破坏。

* 数据库安全策略？安全管理策略、信息流控制策略、访问控制策略（分为集中式控制和分布式控制）

数据库安全策略是组织、管理、保护和处理敏感信息的规则，包括安全管理策略、信息流控制策略和访问控制策略。

安全管理策略的目的是定义用户共享数据和控制它的使用。该目的可由拥有者完成，也可由管理员实现。这两种管理的区别在于，拥有者可以访问所有可能的数据类型，而管理员具有控制数据的能力。

信息流控制策略主要考虑如何控制一个程序去访问数据。安全级别高的可以访问安全级别低的数据，但安全级别低的不能访问安全级别高的数据；当写入时，安全级别高的数据不能写入安全级别低的库中。

访问控制策略是数据库安全策略的重要组成部分，一般分为：集中式控制和分布式控制。

* 数据库系统的访问控制策略？最小特权策略、粒度适当策略、最大共享策略、开放和封闭系统策略、按访问类型划分的控制策略、与内容相关的访问控制、上下文相关的访问控制策略、与历史相关的访问控制。
* 数据库系统安全机制？身份认证机制、访问控制、加密机制、审计机制、推理控制与隐通道分析、安全恢复机制。

**2、数据库系统加密技术**

* 所采用的加密技术满足的要求？

（1）对数据库加密不应影响系统原有的功能，仍能保持数据库对数据操作的灵活性和简便性。

（2）加解密的速度必须足够快，特别是对解密的速度要求更高。

（3）加密机制在理论上和计算上都具有足够的安全性。

（4）加密后的数据库存储量没有明显增加，不能破坏字段长度的限制.

（5）加密后的数据有较强的抗攻击能力，应该能够满足DBMS定义的数据完整性约束，解密时能识别对密文数据的非法篡改。

（6）加解密对数据库的合法用户是透明的。

（7）具有合理的密钥管理机制，保证密钥存储安全，使用方便、可靠。

* 加密方法及其存在的问题？库内加密和库外加密

库内加密：

（1）需要创建一些DMBS内核加解密原语，还有对应的数据库加解密的数据库定义语句、带有加解密实现的数据库操纵语句；

（2）对数据库管理系统的修改是一项浩大的工程，其内部模块之间的分配关系很复杂，修改结构往往会影响系统的稳定性，从而引发无法预知的风险；

（3）应用的加密算法只能局限于DBMS提供的算法，缺乏灵活性；

（4）用于加密的密钥库通常也存放在DBMS系统文件中，密钥的安全和数据库的安全都依托于数据库自身的安全机制。

库外加密：加密后的数据库文件无法识别；密钥无法根据需求合理产生和管理；整个数据库文件使用一个密钥，一旦密钥丢失，数据库将受到重大安全威胁；频繁加解密导致密钥暴露的可能性增大；效率低下。

* 数据库系统加密的粒度及其效率？

（1）数据库级加密：将每个数据库文件作为加密系统的输入。容易实现，但査询效率低。

（2）表级加密：与前者相比，节省系统资源，改善查询性能。但需要修改DBMS内核，风险大。

（3）记录级加密：把数据表中的一条完整记录加密。加密的粒度更细，灵活性更高，更好的查询性能，但工作量较大。

（4）字段级加密：对一个属性值加密，又称为属性加密或域加密。灵活度更高，但会被通过对比明文攻击获取密文信息。

（5）数据项级加密：指加密每个字段记录的数据元素，是最小粒度。具有最高灵活度和最高安全强度。但密钥管理、更新较为繁琐。

**3、数据库系统审计**

* 主要功能？安全审计数据产生、安全审计自动响应、安全审计分析、安全审计浏览、安全审计事件选择、安全审计事件存储。
* 安全审计系统建设目标

（1）有效获取所需数据是安全审计的第一步；

（2）提供事件分析机制，具备评判异常、违规的能力；

（3）保证审计功能不被绕过；

（4）有效利用审计数据；

（5）审计系统的透明性.

**4、数据库备份与恢复技术**

* 事务的四大特性？

事务是指数据库系统的逻辑工作单元执行的一系列操作，事务具有四

大特性：原子性、一致性、隔离性、持久性。

* 故障类型？

事务故障

由于某种原因，事务运行过程中没有运行到正常的终止点，此时系统会强迫发生故障的事务终止运行。原因可能是运算溢出、发生死锁等，破坏了事务原子性。

 系统故障

由于某种原因，造成整个系统的正常运行突然停止，致使所有正在运行的事务都以非正常方式终止的任何事件，都称为系统故障，如：CPU故障、断电等。破坏了事务原子性和持久性。

 介质故障

介质故障又称为硬故障，是指外部存储设备发生故障，从而造成数据部分或全部丢失。破坏了事务原子性和持久性。

* 数据库系统恢复方法

DBMS维护一个日志文件来记录事务对数据库的更新操作，以帮助事务的恢复。内容包括：事务的开始标记、事务的结束标记、事务的所有更新操作。对数据库的修改操作包含两部分：执行修改数据库的操作，将修改操作记录到日志中。这两步需要遵循“日志先写”的原则。

事务故障的恢复

在不影响其他事务运行的情况下，强行回滚该事务，具体为：利用日志文件撤销（UNDO）此事务已对数据库进行的修改，通常的做法是逆向扫描日志文件，将修改前的值写入数据库。

系统故障的恢复

让所有非正常终止的事务回滚，强行撤销所有未完成的事务，重做（REDO）所有已提交的事务，从而保证数据库恢复到一致性状态。重做过程是正向扫描日志。将修改后的值写入数据库。

介质故障的恢复

介质故障的恢复不仅要使用日志，还要借助于数据库备份。数据库备份，又分为静态备份和动态备份，不同的备份方法，将数据恢复到一致性状态的方式有所不同。

**第八章知识点**

**1、概述**

* 概念和内容？

入侵是指任何试图破坏或危及信息系统资源的完整性、机密性和可用性的行为。一旦信息系统与网络连接，其被攻击者入侵的危险就可能存在。

入侵检测就是对入侵行为的发现，是一种试图通过观察行为、安全日志或审计数据来检测入侵的技术。

入侵检测内容：试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户的泄露、独占以及恶意使用资源等。、

入侵检测检测的是威胁，漏洞扫描是扫描脆弱性。

* 入侵检测的模型？

主体：在目标系统上操作的实体。如：用户、进程等。

对象：系统所管理的资源。如：文件、设备等。

审计记录：主体对对象实施操作时所产生的数据，由一个六元组组成<Subject,Action,Object,Exception-Condition,Resource-Usage,Time-Stamp>。

活动简档：用于保存主体正常活动的有关信息，具体实现依赖于检测方法，可利用方差、马尔可夫链等方法实现。

异常记录：记录异常事件发生的情况，有一个三元组组成<Event,Time-Stamp,Profile>。

规则集处理引擎：结合活动简档，分析收到的审计记录，调整内部规则或统计信息，在判断有入侵时采用的相应措施

* IDS的优缺点？

 优点：

提高信息安全体系中其他部分的完整性；

提高系统的监控能力：能够从入口点到出口点跟踪用户的活动；能够识别和汇报文件的变化；能够侦测系统配置错误并纠正；能够识别特殊攻击类型并向系统安全管理员汇报，进行自动防御。

 缺点：

无法弥补差的认证机制；不能弥补网络协议的弱点；不能弥补系统服务质量或完整性的缺陷；如果没有人的干预，不能管理攻击调查；不能指导安全策略的内容；不能分析一个堵塞的网络。

* 入侵检测系统的分类？

1、根据检测的对象分类：基于主机的入侵检测系统；基于网络的入侵检测系统；混合入侵检测系统。

2、根据分析方法分类：异常入侵检测系统；特征入侵检测系统；协议分析入侵检测系统。

3、根据工作方式分类：在线检测系统；离线检测系统。

4、根据检测结果分类：二分类入侵检测系统；多分类入侵检测系统。

5、根据响应方式分类：主动入侵检测系统；被动入侵检测系统。

6、根据系统模块的分布方式分类：集中式入侵检测系统；分布式入侵检测系统。

过程：入侵信息收集，入侵信号分析，入侵检测响应。

* 入侵检测系统收集的信息？系统和网络日志、目录和文件中的异常改变、程序执行中的异常行为、物理形式的入侵信息
* 入侵信号的分析方法？模式匹配、统计分析、完整性分析（主要是关注某个文件或对象是否被修改，通常采用消息摘要的方式识别。）
* 入侵检测相应类别？主动响应和被动响应

通知系统安全管理员，系统正在遭受不良行为的入侵（被动响应）；采取一定的措施阻止入侵行为的继续（主动响应），如：断开网络连接、杀死可疑程序，甚至对攻击系统实施反击。

**2、基于主机的入侵检测系统**

* 审计数据的获取方法？直接获取和间接获取

直接监测获取：从数据的产生或从属的对象直接获得数据。

间接监测获取：从反映被监测对象行为的某个源获取数据。

直接监测获取数据的方式优于间接监测获取数据方式：

（1）间接监测获取的数据可能在入侵检测系统使用前已经被篡改了。

（2）间接数据源记录的数据不是为检测入侵用的，入侵检测需要的一些事件可能没有被数据源记录，而且间接数据源并不能访问被监测对象的内部信息。

（3）间接数据源记录的数据量比较大，入侵检测系统需要从中筛选出有用的信息，工作量巨大；而直接监测获取的数据是那些需要的信息，数据量小，因此对资源消耗就小。

（4）由于间接监测获取的数据是从监测对象的某个源中获取，因此，与直接监测获取的数据相比，存在较大的延时。

* 审计数据预处理的指标？数据集成、数据清洗、数据融合、数据简化、数据变换

**3、基于网络的入侵检测系统**

* 包捕获机制的原理和方法

包捕获机制是依赖于操作系统的，从广义的角度看，一个包捕获机制包含三个主要部分：最底层是针对特定操作系统的包捕获机制，中间层是包过滤机制，最高层是针对用户程序的接口。

包捕获机制是在数据链路层增加一个旁路处理器，对发送和接收的数据包进行缓冲和过滤等处理，最后直接送到应用程序。

包捕获机制不影响网络协议栈对数据包的处理，它只是对所捕获的数据包根据用户的要求进行筛选，最终把满足过滤条件的数据包传递给用户程序。

包过滤操作既可以在用户空间执行，也可以在内核空间执行，但必须注意到数据包从内核空间拷贝到用户空间的开销很大，如果能够在内核空间进行过滤，会极大地提高捕获入侵行为的效率。

作用：（1）包捕获机制是从数据链路层旁路数据包，不影响数据包的正常处理；（2）数据包捕获机制对于用户和应用程序是透明的；（3）可以根据用户的需要对数据包头和协议进行过滤。

局限性：（1）所有的程序都是针对操作系统开发，可移植性差；（2）如果在内核空间执行所有操作，速度快，但程序开发复杂；如果在内核空间采集数据，用户空间处理数据，则浪费CPU周期。

* BPF模型

BPF模型是基于BSD系统的包过滤模型，它使用基于寄存器的过滤算法，在内核态处理数据包，使其性能和效率得到大幅提高。

网卡设置为混杂模式。

**4、入侵检测系统的评估**

* 入侵检测系统的性能指标？准确性、处理性能、完备性、容错性、及时性
* 入侵检测系统的测试评估？功能性测试、性能测试、产品可用性测试

**第九章知识点**

**1、可信计算的概念**

* 什么是可信？

 可信是指值得信任，一个系统可信是指系统的运行（或输入输出关系）符合预期的结果，没有出现未预期的结果或故障。

TCG的定义：如果一个实体的行为总是以预期的方式达到既定目标，那么它是可信的。

ISO／IEC15408的定义：一个组件、操作或过程的可信是指在任意操作条件下是可预测的，并能很好地抵抗应用程序软件、病毒以及一定物理干扰所造成的破坏。

信任的属性：

信任具有二重性，既具有主观性又具有客观性。

信任不一定具有对称性，即A信任B不一定就有B信任A。

信任可度量，也就是说信任的程度可以测量，可以划分等级。

信任可传递，但不绝对，而且在传播过程中有损失。

信任具有动态性，即信任与与环境(上下文)和时间等因素相关。

* 可信计算需要达到的要求？

验证用户的身份：验证使用者的合法身份，可以使用该系统；

验证平台软硬件配置的正确性：使用者可以信任平台的运行环境，软硬件配置没有问题；

 验证应用程序的完整性和合法性：在平台上运行的应用程序是可信的，是正版软件且未受破坏；

 平台之间的可验证性：在网络环境下运行的多个平台之间是可以相互信任的，即这些平台本身各自可信，且可以合法地相互访问，相互通信不存在安全问题。

* TCG的可信计算和微软的可信计算的安全属性？

TCG联盟制定了可信计算规范，提出了基于可信计算平台模块（TPM）的可信计算平台（TCP）体系结构。主要定义了可信计算的三个安全属性：

可鉴别性（Authentication）：信息系统的用户可以认证与他们进行通信的对象身份。

完整性（Integrity）：用户能够确保信息在传输和保存过程中不会被窜改或伪造。

机密性（Privacy）：用户相信系统能保证其信息的私密性不被泄漏。

在2002年，微软发布的“可信计算”白皮书中，从实施（Execution）、方法（Means）、目标（Goals）三个角度对可信计算进行了概要性的阐释。其目标包括四个方面：

安全性（Security）：用户希望系统受到攻击后具有恢复能力，而且能够保护系统及其数据的机密性、完整性和可用性；

机密性（Privacy）：用户能够控制与自己相关的数据不会泄密，并按照信息平等原则使用数据；

可靠性（Reliability）：用户可在任何需要服务的时刻获得服务；

完整性（Integrity）：强调服务提供者以快速响应的方式提供负责任的服务，且服务在传输和保存过程中不会被窜改或伪造。

* 什么可信根？

可信根是系统的安全基础也是安全起点，在可信网络环境中所有安全设备都信任该可信根。可信应用将会从下层获得安全支撑，而非可信应用可以运行于可信系统之上，但不能获得安全支撑。

* 可信计算的基本功能？完整性度量、存储和报告；平台证明（只用于远程调用，本地不需要证明）；受保护能力

**2、可信计算技术**

* 可信平台的可信根有哪些？

TCG认为一个可信平台必须包含三个可信根：

可信度量根（Root of Trust for Measurement，简称RTM）

可信存储根（Root of Trust for Storage，简称RTS）

可信报告根（Root of Trust for Report，简称RTR）

* TPM的基本结构和工作模式？

第一阶段：TPM是平台可信的起点，可信信息系统以它为信任根构建可信的计算环境。

第二阶段：平台上电后，首先TPM芯片验证当前底层固件的完整性，如正确则完成正常的系统初始化。

第三阶段：由底层固件依次验证BIOS和操作系统的完整性，如正确则正常运行操作系统，否则运行停止。

第四阶段：利用TPM内置的加密模块生成系统所需要的各种密钥。

TPM至少需要具备四个主要功能：对称/非对称加密、安全存储、完整性度量和签名认证。

内核模式：运行TPM设备驱动和TPM的核心组件；只有在管理员授权下才能修改其中运行的代码

用户模式：根据用户的要求来加载和执行应用程序和服务；用户模式有两类进程：系统进程和用户进程。

* EK和AIK的关系？

EK密钥由TPM芯片生产厂商生成，是TPM芯片的唯一标识，在理想状态下，TPM内部保存着可信第三方颁发的EK证书用以证明EK的合法性。EK是重要的私有信息，用EK加密或签名数据，攻击者可能会从被加密的数据中获取EK的相关信息而攻击TPM。平台身份密钥AIK由此产生。利用AIK密钥可以进行签名与加密等操作。AIK密钥由平台所有者产生，保存在TPM、内部或外部。平台身份证书由可信第三方签发，用以证明AIK密钥的合法性。AIK可以看作是EK的“别名”，EK只有一对，但EK可以对应多对AIK，之后，平台(或用户)可以针对不同应用或不同时间使用不同的AIK证书来表征平台身份可信性，利用AIK也可以实现与EK相比更大的新鲜度。

**3、信任链技术**

* 信任链的度量过程？PCR值的操作方法及其特点？静态度量和动态度量的区别？

信任链：CRTM→BIOS→OSLoader→OS→Applicatons

信任链的度量过程：

（1）当系统加电以后，CRTM度量BIOS的完整性。

（2）如果BIOS可信，则可信的边界将从CRTM扩展到CRTM+BIOS。于是执行BIOS。

（3）BIOS度量OSLoader。

（4）如果OSLoader可信，则可信的边界扩展到CRTM+BIOS+OSLoader，执行操作系统的加载程序。

（5）OSLoader在加载操作系统之前，首先度量操作系统的完整性。

（6）如果操作系统可信，则可信边界扩展到CRTM+BIOS+OSLoader+OS，加载并执行操作系统。

（7）操作系统启动后，由操作系统度量应用程序的完整性。

（8）如果应用程序可信，则可信边界扩展到CRTM+BIOS+OSLoader+OS+

Applications，操作系统将加载并执行应用程序。

TPM只允许两种操作来修改PCR的值：重置操作和扩展操作。

重置操作发生在机器断电或者重新启动之后，PCR的值自动重新清零（但TCG 1.2新引入的寄存器除外）。

只能通过扩展操作来改变PCR的内容。扩展操作是不可交换的，即先扩展度量值A再扩展度量值B所得到的PCR值跟先扩展B再扩展A的结果是不同的。

理论上PCR能够记录一个无限长的度量值序列，这个度量值序列反映了系统状态的变迁。

如果扩展序列中的某个度量值被改变了，那么后续的度量序列都会受到影响。

静态可信度量的起点是 BIOS；静态度量的可信根是CRTM ；动态可信度量的起点是CPU。

信任度量是在平台启动时进行的一次性完整性验证，此时作为可信度量根的 BIOS 在平台的运行生命周期内执行一次，且度量的实体资源仅限于操作系统及其加载之前的软硬件，这种度量被称为静态度量，它没有度量运行过程中加载的软件，因此无法保证系统运行时的安全。

动态可信度基于CPU中的动态可信根，以指令执行的方式通知TPM进行信任度量。因此动态可信度量可以抵御引导装载程序（BootLoader）的漏洞，以及针对 BIOS 的攻击，但还存在 TPM 被重置的攻击。

有了DRTM之后，TPM可以在任何时候执行度量，重新构建平台的信任链，而不需要重启整个平台。这种重新构建信任链的过程，既可以在平台启动时完成，也可以在平台启动后运行的任何时候完成，从而重新创建可信计算环境，但 DRTM 技术只是实现了信任链的多次度量，其度量的内容还是软件的数据完整性，并不是软件的可信性，因此，DRTM 技术同样没有解决软件可信的问题。

**第十章知识点**

**1、信息系统安全管理概述**

* 概念及其五要素？

概念：信息系统安全管理指通过计划、组织、领导、控制等环节来协调人力、物力、财力等资源，从而保证组织内的信息系统以及信息处理的安全。

五要素：管理的主体、管理的客体、管理手段、管理环境、管理目标。

* 总体管理目标及其本质？

总体管理目标：是保证系统中的信息在整个生命周期内都是安全的。

信息系统安全管理的本质：信息安全管理，其核心是风险管理。

* 宏观管理和微观管理？

宏观管理（国家层面，属于政府管理范畴）

战略方针：即政府制定的信息安全战略方针，如：网络强国战略，为信息安全提出宏观的方向、任务和目标。

各项政策：即根据战略方针制定的各项政策，包括：等级保护、风险评估、灾难恢复、应急响应、信息安全学科设置等，政策是瞄准方向、完成任务和达到目标的措施。

法律和法规：即制定体现客观规律、社会利益和国家意志的法律、法规，包括：保密法、等级保护规范、信息安全条例、信息安全法规等，它限制和约束机构和个人的行为。

标准：指导技术和管理行为的标准。

微观管理（属于机构管理范畴）

策略：即机构根据其信息化目标所需要的安全保障来制定安全管理策略。

规章：即将策略具体化、明确化为可操作的内容。

制度：即保证规章能够有效执行的手段。

实践：即执行信息安全管理的相关规定，确保管理策略、规章、制度能够规范化的执行

* 安全管理的原则？基于安全需求原则、主要领导负责原则、全员参与原则、系统方法原则、持续改进原则、依法管理原则、分权和授权原则、选用成熟技术原则、分级保护原则、管理与技术并重原则、自保护和国家监管结合原则
* 信息系统安全标准的重要性？

信息系统安全标准是信息系统安全保障体系的重要组成部分，是政府管理范畴的一个重要内容，也是信息系统安全微观管理的重要依据之一。但是由于信息系统安全标准不同于其他标准，它关系到一个国家的利益和安全，因此，任何国家都不会过分相信和依赖他人，总是通过自己国家的组织和专家制定出自己可以信赖的标准来保护国家利益和安全。

**2、信息系统安全管理体系**

* 目标和范围？

信息系统安全管理理论是基于风险的信息安全管理体系。而风险是与生俱来的，只要机构需要依靠信息系统来维持业务运作，机构就必须面对信息系统所带来的信息安全风险。信息安全是相对的，同样承载信息的系统安全也是相对的，这主要是因为机构在建立系统安全防护体系时需要考虑成本和效益之间的平衡，同时所采用的安全技术（如密码技术）本身也存在着缺陷，因此，信息系统安全建设的宗旨之一就是在综合考虑成本和效益的前提下，通过恰当、足够、综合的安全措施来控制风险，使残余风险降低到可以被机构接受的程度，既不能忽视保护，也不能过保护。在这种情况下，信息系统安全管理要做的就是如何利用管理的手段，控制风险。

* 安全管理策略？

基本的安全管理策略；较完整的安全管理策略；体系化的安全管理策略；强制保护的安全管理策略；专控保护的安全管理策略。

* PDCA模型的原理？

依据ISO/IEC 27001标准（信息安全管理体系ISMS），采用“计划（P）-实施（D）-检查（C）-处置（A）”（PDCA）模型架构所有ISMS的流程。

1、计划（Plan）——P阶段

2、实施（Do）——D阶段

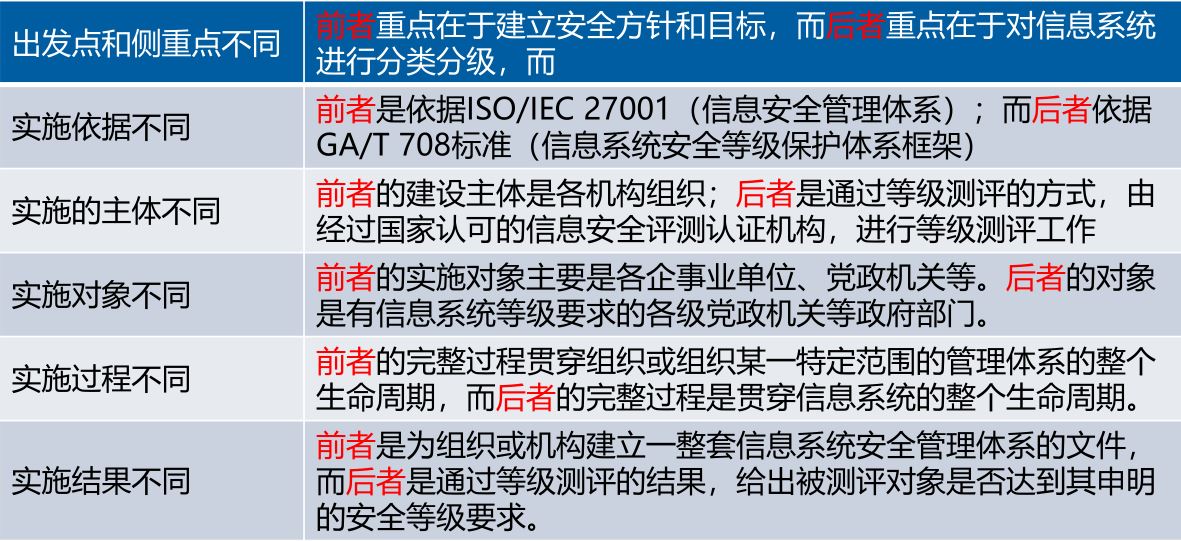
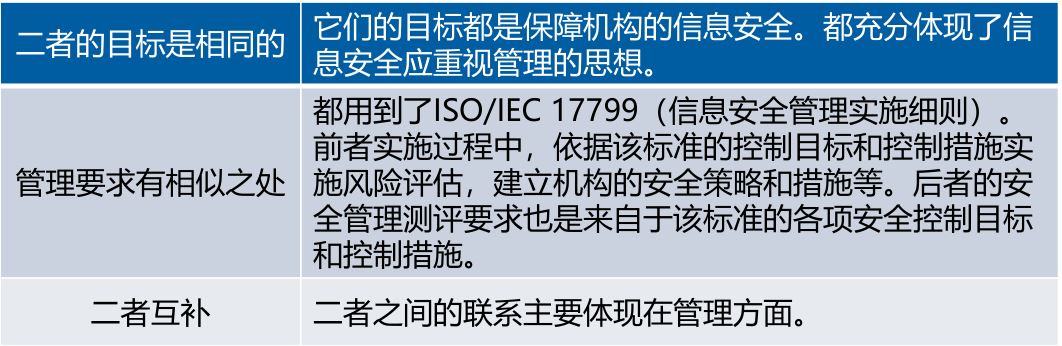
3、检查（Check）——C阶段

4、处置（Act）——A阶段

* 安全管理体系和等级保护的异同？

信息系统安全管理体系建设过程是将信息系统安全管理体系、等级保护和

风险评估三者进行融合的过程。



**3、信息系统安全管理措施**

* 信息系统安全管理措施的概念？

信息系统安全管理措施主要是针对安全要求和风险，选择和实施合适的控制，以确保将风险控制到一个可以接受的程度。

* 安全控制措施主要三种类型？管理控制、技术控制和物理控制
* 物理安全管理、系统安全管理、运行安全管理、数据安全管理和人员安全管理、技术文档安全管理

人员安全管理：

（1）安全组织的建设：建立安全组织，完善管理制度，建立有效的工作机制；人员业务培训、安全意识培训和教育。

（2）人员安全审查：从人员的安全意识、法律意识和安全技能等方面进行审查，遵循“先审查，后上岗，先试用，后聘用”原则。

（3）安全培训和考核：机构应定期对从事操作和维护信息系统的工作人员进行培训以及业务和思想品质考核。

（4）签订安全保密合同：对违反保密合同的人员应进行相应的处理，触犯法律的应追究其法律责任。

（5）离岗人员的安全管理：人员管理必须有关于人员调离的安全管理制度。

（6）人员安全管理的原则：职责分离原则、岗位轮换原则、最小特权原则、强制休假原则、限幅级别。

**第十一章知识点**

**1、信息系统安全风险评估概述**

* 信息系统安全风险评估的概念？

信息系统安全风险评估是依据有关信息系统安全技术与管理标准，对信息系统及由其产生、处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

* 风险评估的目的和时机？

确定系统脆弱性和威胁源的分布；确定这些威胁发生的可能性；分析威胁发生后对系统造成的危害到底有多大，以确定相应的级别；确定敏感、重要资产在威胁发生后的损失。

信息系统安全风险评估是信息系统建设的起点和源头。

通过安全风险评估，可全面、准确地了解组织的安全现状，发现系统的安全问题和可能的危害，从而确定信息系统的安全需求。

信息系统安全风险是以安全需求为主导的，但在评估过程中需要突出重点。

信息系统安全风险评估需要考虑具体的时机，一般情况如下：

1、在设计规划或升级信息系统时；

2、需要增加新的应用或新的扩充时；

3、发生安全事件后；

4、组织发生结构性变动时；

5、按照某些规定或特殊要求，对信息系统的安全进行评估时。

* 风险评估的原则？

标准性原则：遵循GB/T 20984-2007 信息安全技术 信息安全风险评估规范。

关键业务原则：信息系统安全风险评估应以被评估组织的关键业务作为评估工作的核心，把涉及这些业务的相关网络与系统作为评估的重点。

可控性原则：服务可控性；人员与信息可控性；过程可控性；工具可控性。

最小影响原则：首先保障业务系统的稳定运行，而对于需要进行攻击性测试的工作内容，需与用户沟通并进行应急备份，同时选择避开业务的高峰时间进行。

**2、风险评估方法**

* 风险评估的基本要素与其属性之间的关系？

安全风险评估涉及的基本要素包括资产、威胁、风险、脆弱性和安全措施。风险评估围绕着这些基本要素展开，在对基本要素的评估过程中，需要充分考虑业务战略、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各种属性。

风险评估的基本要素与其属性之间的关系

（1）业务战略的实现对资产具有依赖性，依赖程度越高，要求其风险越小；

（2）资产是有价值的，组织的业务战略对资产的依赖程度越高，资产的价值就越大。

（3）风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成为安全事件；

（4）资产的脆弱性可能暴露资产的价值，资产具有的弱点越多则风险越大；

（5）脆弱性是未被满足的安全需求，威胁利用脆弱性将危害资产；

（6）风险的存在和对风险的认识，导出安全需求；

（7）安全需求可通过安全措施得以满足，需要结合资产价值考虑实施成本；

（8）安全措施可以抵御威胁，降低风险；

（9）残余风险有些是由于安全措施不当或无效造成的，而有些则是在综合考虑了安全成本与效益后未去控制的风险；

（10）残余风险必须密切关注，它可能在将来的某个时刻诱发新的安全事件。

* 风险评估包含哪些环节？

风险评估一般包含识别风险、分析风险、评价风险和处理风险等环节。

* 风险分析涉及哪些要素和主要内容？

风险分析要涉及资产、威胁、脆弱性等三个基本要素，每个要素有各自的属性，资产的属性是价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。

风险分析的主要内容：

（1）对资产进行识别，并对资产的价值进行赋值；

（2）对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；

（3）对脆弱性进行识别，并对具体资产脆弱性的严重程度赋值；

（4）根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

（5）根据脆弱性的严重程度及安全事件所作用的资产价值，计算安全事件的损失；

（6）根据安全事件发生的可能性及安全事件出现后的损失，计算安全事件一旦发生对组织造成的影响，即风险值。

* 风险评估的实施流程？风险评估的准备、资产识别、威胁识别、脆弱性识别、已有安全措施的确认、风险分析、风险评估文档记录

1、风险评估准备：确定风险评估的目标；确定范围；组建团队；系统调研；确定依据；制定方案；获得支持。

2、资产识别：

资产分类：保密性、完整性和可用性是评价资产的三个安全属性，分类是进行下一步的风险评估的基础。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者灵活把握。

资产赋值：保密性赋值；完整性赋值；可用性赋值；资产重要性等级。资产价值应依据资产在保密性、完整性和可用性上的赋值等级，经过综合评定得出。综合评定方法可根据自身的特点，选择对资产保密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果。也可以根据资产保密性、完整性和可用性的不同等级对其赋值进行加权计算，得到资产最终赋值结果。

3、威胁识别：

威胁分类：威胁可以通过威胁主体、威胁的对象、动机、途径等多种属性来描述。威胁的因素可分为人为因素和环境因素。威胁作用的形式可以是对信息系统直接或间接的攻击。

威胁赋值：判断威胁出现的频率是威胁赋值的重要内容，评估者应根据经验或有关的统计数据来进行判断。涉及三方面内容：以往安全事件报告中出现过的威胁及其频率的统计；实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

4、脆弱性识别：以资产为核心；脆弱性严重程度可以进行等级化处理。等级数值越大，脆弱性严重程度越高。

５、已有安全措施确认：确认是否真正地降低了系统的脆弱性，抵御了威胁。安全措施可以分为预防性安全措施和保护性安全措施。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少安全事件发生后对组织或系统造成的影响。

6、风险分析：风险结果的判定；风险处理计划；残余风险评估。

* 风险计算的方法：相乘法、矩阵法

**3、风险评估工具**

* 风险评估工具的选择原则？

实际需要原则；试用原则；实用原则；满足脚本数量与更新速度要求；支持不同级别的入侵检测。

* 风险评估工具的种类？

基于信息安全管理标准或指南的风险评估工具；基于知识库的风险评估工具基于定性或定量算法的风险评估工具。

**4、等级保护**

* 等级保护模型？

针对安全目标，参照GB17859-1999 计算机信息系统安全保护等级划分准则，信息系统的五个安全等级分别为：

 第一级 用户自主保护级（对应C1级）

 第二级 系统审计保护级（对应C2级）

 第三级 安全标记保护级（对应B1级）

 第四级 结构化保护级（对应B2级）

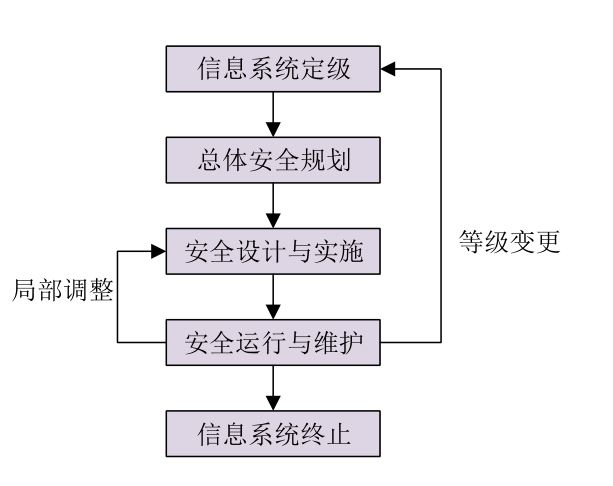
 第五级 访问验证保护级（对应B3级）

信息系统基本安全需求包含基本技术要求和基本管理要求。基本安全技术需求包含物理安全、网络安全、主机安全、应用安全和数据安全等5个层面。基本管理要求包括安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等5个方面。

* 等级保护应遵循的原则？

自主保护原则、重点保护原则、同步建设原则、动态调整原则

* 等级保护的基本流程？



* 等级划分的基本思想？

在资产价值级别与威胁级别相同的情况下，该级别则为信息系统（安全域）的安全保护等级；在资产价值级别大于威胁级别的情况下，以威胁级别作为信息系统（安全域）的安全保护等级；在资产价值级别小于威胁级别的情况下，以资产价值级别作为信息系统（安全域）的安全保护等级。