信息安全

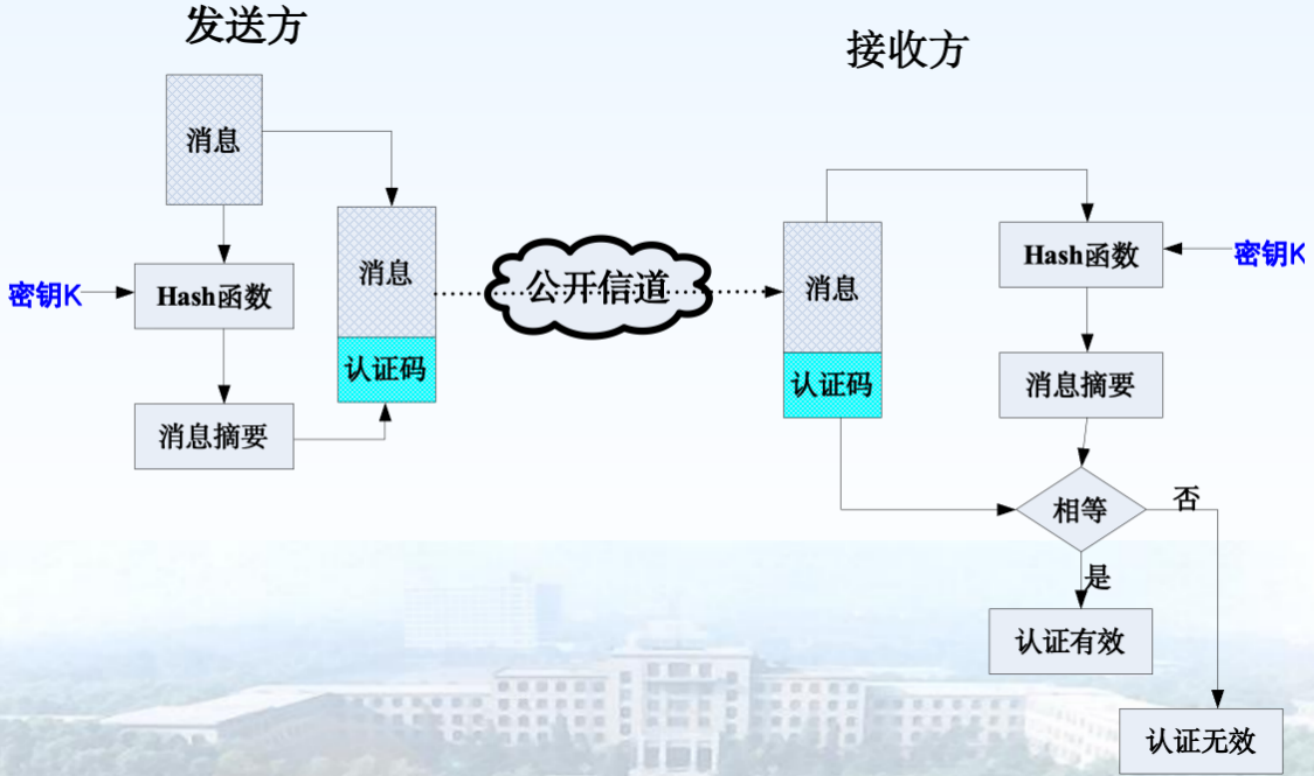
第二章

第四节 认证理论与技术

认证的目的是什么？主要包括哪些方面的认证?

（1）验证信息的发送者是真实的，而不是冒充的，称为实体认证。包括信源、信宿等的认证与识别；
（2）验证消息的完整性，称为消息认证。验证数据在传输过程中未被篡改、重放等。
1.用户认证 2. 设备认证 3. 服务认证 4. 数据认证 5. 软件认证 6. 网络认证 7. 文件认证

图示消息认证的过程。



简述散列函数分组迭代散列算法的层次结构的主要思想与方法。

主要思想是将输入数据分组并迭代地应用散列函数，以生成最终的散列值。

1. 分组：将输入消息分割成固定大小的数据块（通常为512位或1024位），每个数据块称为一个消息块。
2. 初始向量：设定一个初始向量（初始哈希值），作为迭代过程的起点。
3. 迭代过程：
    - 选择一个散列函数（如MD5、SHA-1、SHA-256等），该散列函数将一个消息块和上一轮迭代的散列值作为输入，输出一个新的散列值。

- 将当前的散列值作为下一轮迭代的输入，继续应用散列函数，直到处理完所有的消息块。

4. 最终结果：最后一轮迭代的输出即为最终的散列值。
   这种层次结构的主要思想在于每个消息块的散列值都依赖于前一轮迭代的散列值，形成一个链式结构。

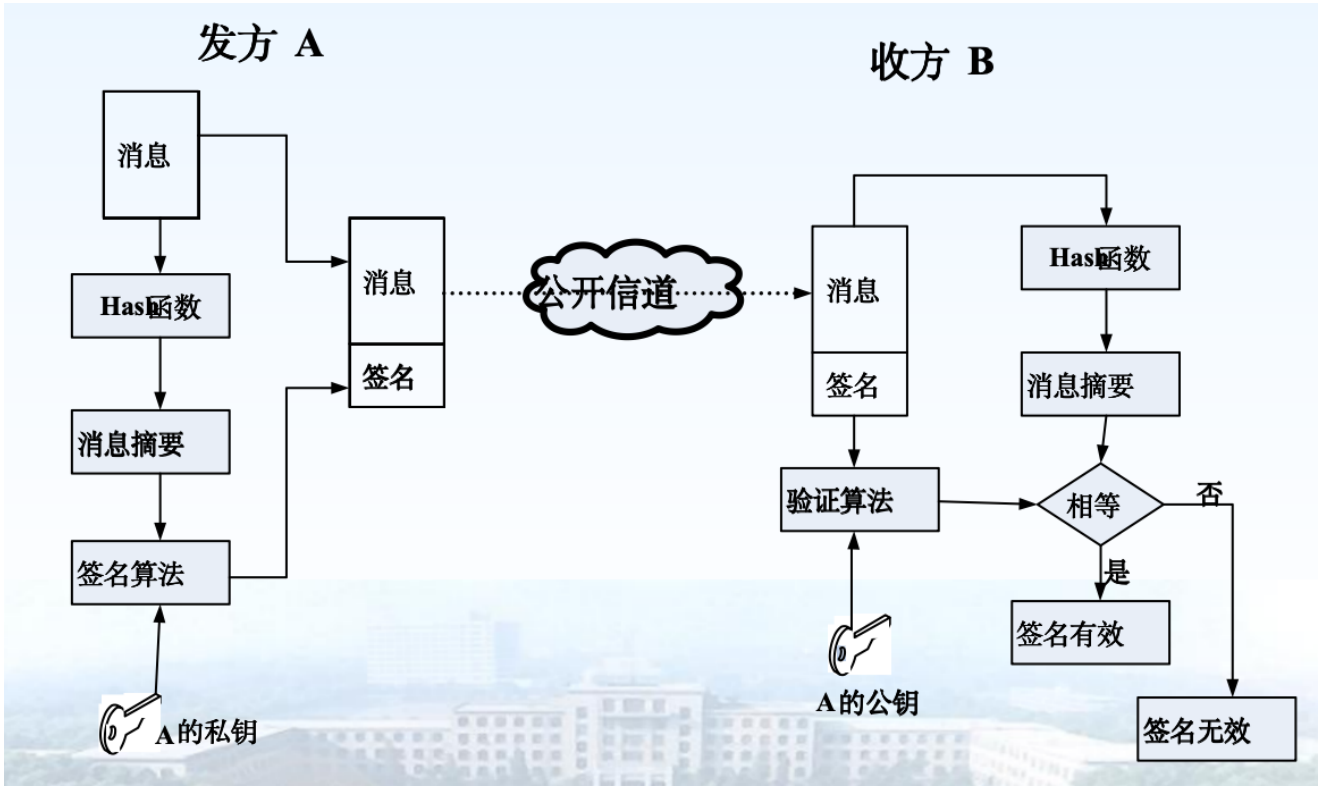
什么叫数字签名？数字签名满足的条件有哪些?

是指附加在某一电子文档中的一组特定的符号或代码，它是利用数学方法和密码算法对该电子文档进行关键信息提取并进行加密而形成的，用于标识签发者的身份以及签发者对电子文档的认可，并能被接收者用来验证该电子文档在传输过程中是否被篡改或伪造。
条件:
收方能够确认或证实发方的签名，但不能伪造；
发方发出签字的消息给收方，就不能否认签发的消息；
收方对已收到的签字消息，不能否认；
第三方可以确认收发双方之间的消息传递，但不能伪造这一过程。

简述数字签名方案的组成。

系统初始化过程：
生成数字签名方案用到的所有参数。
签名生成过程
用户利用给定的算法对消息产生签名s=Sig(m)。
签名验证过程
验证者利用公开的验证方法对给定消息的签名进行验证，得出签名的有效性。Ver(s,m)=0或1

图示数字签名的过程。



说明盲签名的实现原理。

盲数字签名是一种特殊的数字签名，当用户A发送消息m给签名者B时，一方面要求B对消息签名，另一方面又不让B知道消息的内容，也就是签名者B所签的消息是经过盲化处理的。盲签名除具有一般数字签名的特点外，还有下面两个特征：
(1)签名者无法知道所签消息的具体内容，虽然他为这个消息签了名。（匿名性）
(2)即使后来签名者见到这个签名时，也不能将之与盲消息对应起来。（不可跟踪性）
盲变换算法（D.Chaum提出，采用RSA算法）
假设B的公钥为e，私钥为d。
1）A要求B对消息m进行盲签名，选1<k<m，
计算t=mke mod n，将t发送给B
2）B对t签字：td=(mke)d mod n，发送给A
3）A解除盲变换：s=td/k mod n，得 s=md mod n

分析身份认证的主要途径及各种方法的优缺点。

1. 用户名和密码认证：用户提供一个唯一的用户名和相应的密码进行认证。优点是简单易实施和使用，但缺点是容易受到密码泄露、弱密码和暴力破解等攻击。
2. 双因素认证：结合两个或多个不同的身份验证因素进行认证，例如密码与短信验证码、密码与指纹等。优点是提供了更高的安全性，缺点是增加了用户的操作复杂性和使用成本。
3. 生物特征认证：使用个人的生物特征信息进行认证，如指纹、虹膜、面部识别等。优点是唯一性较高且难以伪造，但缺点是设备要求较高，技术成熟度和用户接受度有限。
4. 智能卡认证：使用带有芯片的智能卡进行身份认证，通常使用密码或者密钥进行验证。优点是具有较高的安全性和物理隔离，但缺点是需要专门的硬件设备和管理。
5. 单点登录（SSO）：用户只需进行一次认证，即可访问多个相关联的应用和服务。优点是方便用户操作，减少密码管理负担，但缺点是一旦主凭证泄露，可能导致多个应用受到威胁。
6. 基于公钥基础设施（PKI）的认证：使用数字证书和非对称加密技术进行身份验证。优点是提供了较高的安全性和身份验证的可信度，但缺点是复杂度较高，需要建立和维护密钥基础施。

第五节 公钥基础设施（PKI）

什么是PKI？PKI由哪些部分构成?

PKI（Public Key Infrastructure）是一个用公钥概念与技术来实施和提供安全服务的具有普适性的安全基础设施。PKI公钥基础设施的主要任务是在开放环境中为开放性业务提供数字签名服务。
PKI是一种标准的密钥管理平台，它为网络应用透明地提供加密和数字签名等密码服务所必需的密钥和证书管理。

PKI由证书授权中心CA、注册认证中心RA、证书库、密钥备份及恢复系统、证书作废处理系统、PKI应用接口系统6等部分组成，

CA在PKI中起到什么作用？CA有哪些职责？

作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。CA机构的数字签名使得攻击者不能伪造和篡改证书。它负责产生、分配并管理所有参与网上交易的个体所需的数字证书，因此是安全电子交易的核心环节。

验证并标识证书申请者的身份；
确保CA用于签名证书的非对称密钥的质量；
确保整个签证过程和签名私钥的安全性；
证书材料信息（如公钥证书序列号、CA等）的管理；
确定并检查证书的有效期限；
确保证书主人的标识的惟一性，防止重名；
发布并维护作废的证书表；
对整个证书签发过程做日志记录；
向申请人发通知。 9

什么是公钥证书？公钥证书的用途是什么？公钥证书的主要内容有哪些？

公钥证书是公开密钥体制的一种密钥管理媒介，是一种权威性的电子文档，用于证明某一主体的身份以及公开密钥的合法性。

验证数字签名：消息接收者用发送者的公钥对消息的数字签名进行验证。
加密信息：消息发送者用接收者的公钥加密用于加密数据的密钥，进行数据加密的传送。

1. 版本号
2. 序列号
3. 签名算法标识
4. 颁发者
5. 有效期
6. 主体
7. 公钥信息
8. 扩展字段
9. 颁发者的数字签名

公钥证书的安全性是如何体现的？

证书是公开的，可复制的。
任何具有CA公钥（根证书/CA证书，自签名证书）的用户都可以验证证书有效性
除了CA以外，任何人都无法伪造、修改证书。
证书的安全性依赖于CA的私钥。

公钥证书的有效性验证要验证哪些内容？

使用CA证书验证终端实体证书有效性。
检查证书的有效期，确保该证书是否有效。
检查该证书的预期用途是否符合CA在该证书中指定的所有策略限制。
在证书撤销列表（CRL）中查询确认该证书是否被CA撤销。

第六节 安全协议

什么是安全协议？安全协议有哪些特点？

协议是指两方或多方为完成一项任务所进行的一系列步骤，而每一步必须依次执行，在前一步完成之前，后面的步骤都不能执行。

协议自始至终是有序的过程；
协议至少有两个参与者；
通过执行协议必须能够完成某项任务，达到特定的目标；

安全协议通常由哪些部分构成？

1. 身份认证协议
2. 密钥交换协议
3. 密钥协商协议
4. 数据完整性保护协议
5. 数据加密协议
6. 安全证书和数字签名协议
7. 安全参数协商协议

简述Diffie-Hellman密钥交换协议的主要过程。

1. 参数选择：选择两个大素数p和g作为协议的公开参数。其中，p是一个足够大的素数，g是一个作为底数的小于p的整数。
2. 密钥生成：每个通信方选择一个私密的随机数（私钥），记为a和b。
3. 公开参数交换：通信双方将选定的公开参数p和g发送给对方。
4. 公钥计算：每个通信方使用对方发送的公开参数p和g，以及自己的私钥a或b，计算出自己的公钥。
5. 公钥交换：通信双方将计算得到的公钥发送给对方。
6. 密钥计算：每个通信方使用自己的私钥和对方发送的公钥，计算出一个共享的密钥。
7. 密钥确认：通信双方互相确认计算得到的密钥是否一致。如果一致，则双方都拥有同一个共享密钥。

试分析简化的SET协议是如何保证安全交易的安全支付过程的。

1. 身份验证：数字证书
2. 数据加密：对称加密和公钥加密结合的方式
3. 安全传输：安全套接层协议（SSL/TLS）

4. 数字签名
5. 信任链建立

第三章 信息系统安全体系

安全体系结构提供的主要内容有哪些?

提供的安全服务（安全功能）与有关安全机制在体系结构下的一般描述；
确定体系结构内部可以提供这些服务的位置；
保证安全服务完全准确地得以配置，且在信息系统生命周期中一直维持。

简要说明ISO开放系统互连安全体系结构中的五类安全服务、八类安全机制的内容以及相互的联系。

五类安全服务：

- 鉴别
- 访问控制
- 数据机密性
- 数据完整性
- 抗抵赖

八种安全机制：

- 加密
- 数字签名
- 访问控制
- 数据完整性
- 鉴别交换
- 通信业务流填充
- 路由选择
- 公证

安全服务和安全机制相互关联，通过协同工作来实现系统的安全性。安全服务提供了安全的功能目标，而安全机制则提供了实现这些功能目标的具体技术手段。它们共同构成了ISO开放系统互连安全体系结构的基础框架，为开放系统环境中的安全通信提供了规范和指导。

简述IPSec在传输模式和隧道模式下的主要区别。

传输模式：
端到端的安全
主机必须配置IPSec。
隧道模式：

节点到节点的安全；
主机不必配置IPSec。

说明TLS握手协议的认证模式的主要目标及过程。

1. 身份验证
2. 密钥协商
3. 完整性保护
4. 客户端发送协议版本和加密套件列表
5. 服务器回应协议版本和选择加密套件
6. 客户端验证服务器证书
7. 客户端生成临时密钥
8. 客户端使用服务器的公钥加密临时密钥
9. 服务器解密临时密钥
10. 客户端和服务器计算主密钥
11. 客户端和服务器生成会话密钥
12. 完整性保护和密钥确认

简述信息系统安全体系结构的主要内容。

技术体系：
物理安全技术
系统安全技术
OSI安全技术
相关技术的管理

组织机构体系:
机构
岗位
人事

管理体系:
法律
制度
培训

第四章 访问控制与安全审计

什么是访问控制，访问控制的三要素是什么?

访问控制（Access Control）是一种安全机制，用于限制和管理对系统资源的访问。它确保只有授权的用户、实体或进程能够获取系统资源，并根据其权限级别或角色来执行相应的操作。

主体、客体、控制策略

说明访问控制矩阵的构成以及访问控制的执行过程。

对于任意一个si∈S, oj ∈O, 都存在一个相应的aij ∈A, 且aij =P(si, oj), 其中P是访问权限的函数。
aij代表了si可以对oj执行什么样的操作。

1. 身份认证
2. 授权
3. 访问请求评估
4. 决策
5. 访问执行
6. 审计和监控

分别说明三类访问控制方法的含义及各自的特点。

自主访问控制

- 含义：自主访问控制是一种基于主体拥有者的决策和授权的访问控制方法。主体拥有对自己创建的对象的访问控制权，并可以自主决定谁可以访问对象以及访问权限的级别。
- 特点：
  - 主体拥有控制权
  - 灵活性
  - 分散决策

  强制访问控制
- 含义：强制访问控制是一种基于系统定义的安全策略和标签的访问控制方法。系统根据事先设定的规则来强制限制主体对对象的访问，无论主体的意愿如何。
- 特点：
  - 安全级别高
  - 中央控制
  - 标签和分类
  - 严格限制

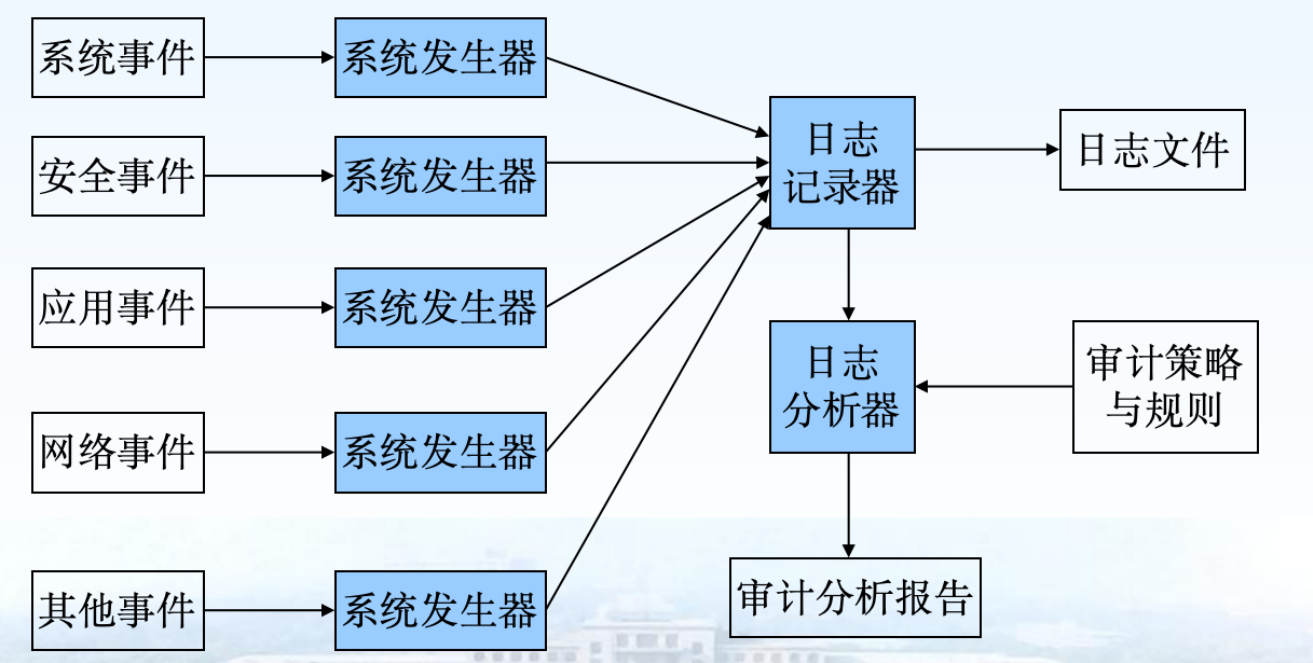
  基于角色的访问控制
- 含义：基于角色的访问控制是一种基于角色和职责的访问控制方法。主体被分配到不同的角色，而角色则被授予特定的权限，主体通过扮演某个角色来获得相应的访问权限。
- 特点：
  - 简化管理
  - 灵活性和可扩展性
  - 职责分离

什么是安全审计？安全审计的目的是什么？

根据一定的策略，通过记录、分析历史操作事件发现和改进系统性能和安全。

审计是对访问控制的必要补充，是访问控制的一个重要内容，审计是实现系统安全的最后一道防线。

简述安全审计系统的构成。



第五章 信息安全管理与安全评估

信息安全管理主要包括哪几个方面?

信息安全政策和法规
信息安全机构和人员管理
技术管理

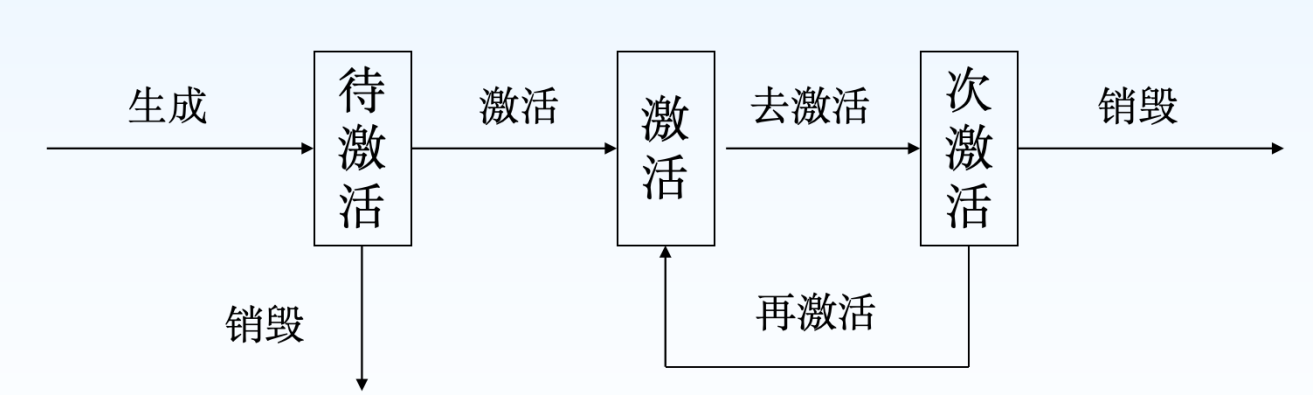
信息安全管理策略遵循的原则有哪些?

（1） 整体性原则
（2） 平衡分析原则
（3）综合性、系统性原则
（4）一致性原则
（5）易操作性原则
（6） 适应性和灵活性原则
（7） 多重保护原则

密钥的安全保护可以从那几个方面实现?

采用密码技术的保护
采用非密码技术的保护
采用物理手段的保护
采用管理手段的保护

简述密钥的生存周期及各状态的特点。



1. 生成（Generation）：密钥的生成是指创建新密钥的过程。在生成阶段，密钥被随机生成，并且通常由密钥生成算法和随机数生成器生成。生成的密钥还没有在任何操作中使用。
2. 存储（Storage）：在存储状态下，生成的密钥会被安全地存储在密钥管理系统（KMS）中或者由安全硬件模块（如HSM）保护。存储状态下的密钥需要受到适当的物理和逻辑安全保护。
3. 分发（Distribution）：在分发状态下，密钥会被传输给需要使用它的实体，例如其他系统、应用程序或用户。分发过程需要确保传输的安全性，通常会使用安全通道或加密技术来保护密钥的传输。
4. 活动（Active）：在活动状态下，密钥已经被接收者接收并开始使用。密钥在活动状态下用于加密、解密、签名或验证等加密操作。密钥在活动状态下需要受到适当的保护，以防止泄露或未经授权的使用。
5. 撤销（Revocation）：当密钥的使用需要终止时，可以将其撤销。撤销密钥可以是计划的，例如密钥过期或需要更新，也可以是紧急的，例如密钥被泄露或存在安全漏洞。撤销后的密钥将无法继续使用。
6. 销毁（Destruction）：在销毁状态下，密钥被永久删除或销毁，不再可用。销毁密钥通常需要在物理上和逻辑上将其完全擦除，以确保无法恢复。

简述可信任计算机系统评价准则(TCSEC)的安全等级划分。

四类八级

- D类：无保护级
  D1级：无保护级
- C类：自主保护级
  C1级：自主安全保护极
  C2级：控制安全保护极
- B类：强制安全保护级
  B1级：标记安全保护级
  B2级：结构化保护级
  B3级：安全域保护级

- A类：验证安全保护级
  A1级 ： 验证设计级
  超A1级

简述我国安全评估标准(GB17859-1999)的安全等级划分及各保护级别对安全功能的要求。

第一级：用户自主保护级
第二级：系统审计保护级
第三级：安全标记保护级
第四级：结构化保护级
第五级：访问验证保护级

级别 / 要求	第一级 用户自主 保护级	第二级 系统审计 保护级	第三级 安全标记 保护级	第四级 结构化 保护级	第五级 访问验证 保护级
自主访问控制	√	√	√	√	√
身份鉴别	√	√	√	√	√
数据完整性	√	√	√	√	√
审计		√	√	√	√
客体重用		√	√	√	√
标记			√	√	√
强制访问控制			√	√	√
隐蔽信道分析				√	√
可信路径				√	√
可信恢复					√

第六章 信息安全实用技术

第一节 防火墙技术

简述防火墙的概念及主要功能

是指一种将内部网和公众网络（如Internet)分开的方法，它实际上是一种隔离技术。

服务控制：确定可以访问的因特网服务的类型；
方向控制：确定特定的服务请求通过防火墙流动的方向；
用户控制：控制用户对特定服务的访问；
行为控制：控制怎样使用特定的服务；

简述包过滤技术的主要实现原理

在网络中适当的位置对数据包实施有选择的通过，选择依据，即为系统内设置的过滤规则（通常称为访问控制表——Access Control List），只有满足过滤规则的数据包才被转发至相应的网络接口，其余数据包则被从数据流中删除。

比较防火墙的主要连接模式的特点

双宿/多宿主机体系结构：一种拥有两个或多个连接到不同网络的网络接口的防火墙。
屏蔽主机体系结构：由包过滤路由器和堡垒主机组成，在这种方式的防火墙中，堡垒主机安装在内部网络上，通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络惟一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。
屏蔽子网体系结构：屏蔽子网防火墙采用了两个包过滤路由器和一个堡垒主机，在内、外网络之间建立了一个被隔离的子网，定义为“非军事区“网络，有时也称做周边网 。

第二节 虚拟专用网技术

简述VPN的概念的特点

是指以公用开放的网络（如Internet, ATM网络等）作为基本传输媒介，通过附加的多种技术而构建出的具有专用网络性能的逻辑网络。
它是一种逻辑上的专用网络，向用户提供一般专用网络所具有的功能，但本身却不是一个独立的物理网络。
（1）虚拟性
（2）专用性

VPN的实现主要用到哪些技术，各种技术在VPN的实现中起到什么作用?

安全隧道技术：将待传输的原始信息经过加密和协议封装处理后再嵌套装入另一种协议的数据包送入网络中，像普通数据包一样进行传输。
认证技术：在正式的隧道连接开始之前需要确认用户的身份，以便系统进一步实施资源访问控制或用户授权
访问控制技术： 由VPN服务的提供者与最终网络信息资源的提供者共同协商确定特定用户对特定资源的访问权限，以此实现基于用户的细粒度访问控制，以实现对信息资源的最大限度的保护。

从应用的角度，VPN可分为哪些类型？每一种类型主要解决哪些问题?

Intranet VPN（内部网VPN）
用于集团的总部和多个分支机构之间；
分支机构网络是集团总部网络的可靠延伸；
Extranet VPN （外联网VPN）
为集团的供货商、重要客户和消费者等商业伙伴提供访问权限；
电子商务是Extranet VPN的一种特殊形式；
Access VPN（远程访问VPN）
为移动用户远程访问集团总部网络提供服务；

第三节 入侵检测技术

简述“入侵”、“入侵检测”、“入侵检测系统”的概念；

入侵：是指对信息系统的未授权访问及（或）未经许可在信息系统中进行操作。这里，应该包括用户对于信息系统的误用。
入侵检测：是指对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程。它通过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。
入侵检测系统(IDS，Intrusion Detection System)，是完成入侵检测功能的软件、硬件及其组合，是一种能够通过分析系统安全相关数据来检测入侵活动的系统。

简述ids入侵检测系统的构成；

信息流收集器：即信息获取子系统，用于收集来自于网络和主机的事件信息，为检测分析提供原始数据；
分析引擎：即分析子系统，是入侵检测系统的核心部分，用于对获取的信息进行分析，从而判断出是否有入侵行为发生并检测出具体的攻击手段；
用户界面和事件报告：即响应控制子系统，这部分和人交互，在适当的时候发出警报，为用户提供与IDS交互和操作IDS的途径；
特征数据库：即数据库子系统，存储了一系列已知的可疑或者恶意行为的模式和定义；

衡量入侵检测系统性能的指标有哪些？各指标的含义是什么？

误报率：检测系统在检测过程中出现误报（把系统的正常行为判为入侵行为的错误）的概率；
漏报率：检测系统在检测过程中出现漏报（把某些入侵行为判为正常行为的错误现象）的概率。

简述入侵检测系统及基本原理；

入侵检测系统（Intrusion Detection System，IDS）是一种安全工具，用于监测和检测计算机网络或系统中的潜在入侵行为。IDS旨在及时发现和响应对网络安全的威胁，以保护系统和数据的安全性。
异常检测
误用检测
特征检测

入侵检测系统通常分为哪两类？主要区别是什么？

基于主机的入侵检测系统（HIDS）
基于网络的入侵检测系统（NIDS）
基于签名的IDS依赖于已知攻击的特征，适用于检测已知攻击模式，而基于行为的IDS关注异常行为模式，可以检测未知的攻击和变种攻击。

简述入侵检测系统的响应机制。

入侵检测系统需要能够处理在分析阶段产生的分析结果，并且概要描述对所检测出的问题作出响应的一些选择模式。
这些选择模式包括：被动响应和主动响应。被动响应就是系统仅仅简单地记录和报告所检测出的问题，而主动响应则是系统（自动地或与用户配合）要为阻塞或影响攻击进程而采取行动。