**第6章 操作系统安全**

一、填空题：

1、信息系统安全的基础是 物理安全 ，操作系统安全是信息系统安全的 核心（或重心） 。

2、操作系统的安全目标是：对系统的用户 身份认证 ，依据安全策略对用户操作进行 访问控制 ， 阻止用户对系统资源的 非法访问 ， 监督系统运行的 安全 ， 保证系统自身的 安全性 和 完整性 。

3、操作系统的存储保护中，数据存储单元可以分为 字 、 字块 、 页面 、或 段 。

4、操作系统的硬件安全机制包括： 存储保护 、 运行保护 和 I/O保护 。

5、TCSEC（橘皮书）标准中，操作系统的安全级别从高到低分为：A1 级、B3级 、B2级 、 B1 级、C2 级、C1级 和 D级。

6、安全访问令牌分为：主令牌 和 模拟令牌。

7、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。

二、选择题：

1、以下属于网络攻击威胁是：（ABCD）

A．病毒；B. 蠕虫；C. 木马；D. 逻辑炸弹；e. 隐蔽通道；天窗

2、以下属于恶意病毒攻击的是（D）

A．病毒；B. 蠕虫；C. 木马；D. 逻辑炸弹；e. 隐蔽通道；天窗

3、以下属于最小特权保护机制的是（ CD ）

A. 将系统用户的角色分为管理员角色和一般用户角色；

B．将系统用户的角色分为root角色和一般用户角色；

C．将系统用户的角色分为系统安全管理员、系统安全审计管理员、系统安全数据复制管理员和一般用户；

D．不给用户分配超过执行任务所需特权以外的权限。

4、windows操作系统访问控制策略包括（ABD）

A. 自主访问控制策略；

B．基于角色的访问控制策略

C. 强制访问控制策略；

D. 基于属性的访问控制策略。

5、安全访问令牌在以下哪个模块中产生（ A ）

A. 本地安全认证（LSA）模块；

B. 安全账户管理（SAM）模块；

C. Netlogon模块；

D. 安全引用监控器（SRM）模块。

6、安全访问令牌可以与以下哪些实体关联（ABD）

A、进程；B. 用户；C. 资源；D. 线程； E. 被访问对象

7、Linux系统的用户口令保存在以下文件中（B）

A. passwd文件；B.shadow文件；C.useradd文件；D. group文件

8、Linux系统中，以下哪些设备采用块设备文件（AB）

A.U盘；B硬盘；C.打印机；D.传真

三、简答题：

1. 病毒和蠕虫的区别？他们的传播途径分别是什么？

要点：（1）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。（2）蠕虫具有传染性和复制功能，但与病毒不同，可以独立存在，无需寄生在某个程序之中。（3）病毒的传播途径是通过感染其他文件进行传播，而蠕虫则是通过系统漏洞传播。

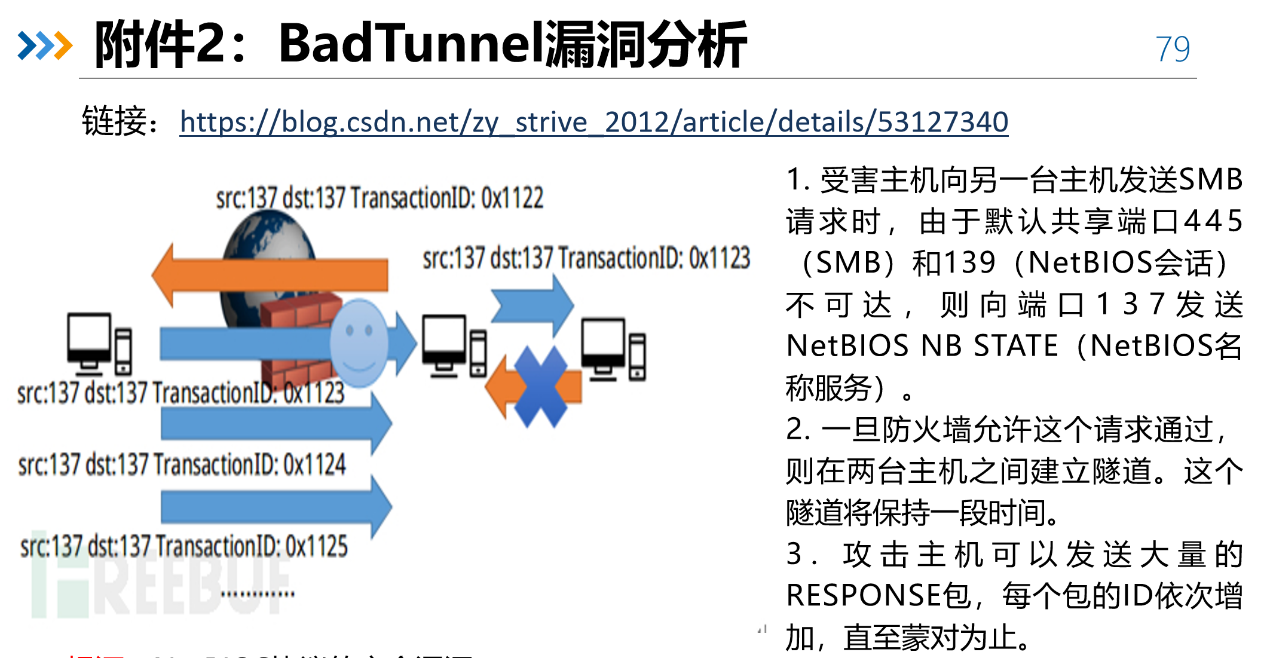
2、简要说明存储管理中，虚拟地址空间和物理地址空间是如何对应的?

要点：通过页表。页表是一种特殊的结构，存放在系统空间的页表区，其中显示的是逻辑地址和物理地址的对应关系。

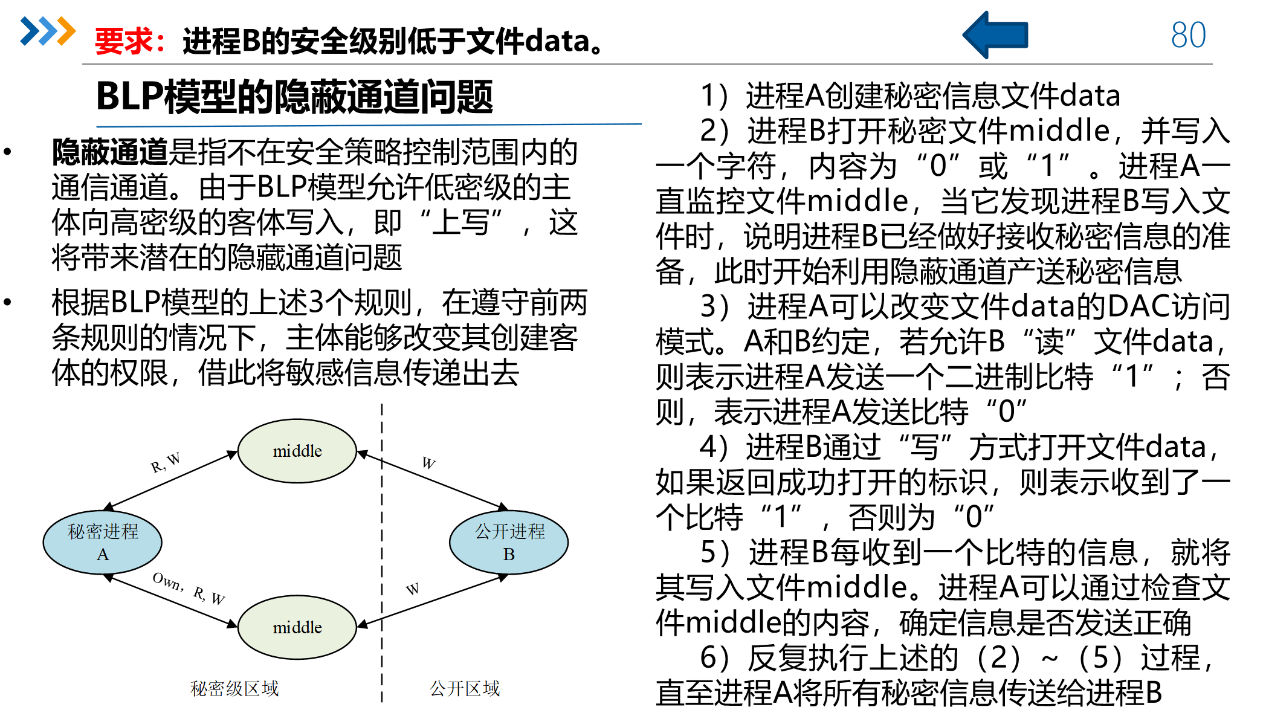
3、隐蔽通道划分成哪两类？每类一个举例，说明工作原理。

要点：（1）隐蔽存储通道；（2）隐蔽定时通道

举例：（1）隐蔽存储通道，说清楚相关工作原理即可



（2）隐蔽定时通道，说清楚相关工作原理即可



4、操作系统的硬件安全机制中，存储单元越小，存储保护的精度越高。那是不是可以认为存储单元越小越好？存储单元过大除了存储保护的精度低外，还会对系统造成什么影响？

要点：（1）不是；（2）虽然存储单元越小，存储保护的精度越高。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，从而造成文件管理复杂；（3）如果存储单元比较大，不仅存储保护的精度低，而且会造成存储的碎片太多，存储空间的浪费。

**5、安全审计时，不仅要记录失败事件，还要记录成功事件，为什么？**

**要点：**（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**。

**6.简述 Android 和 Linux 操作系统安全机制之间的异同。**

**要点：**（1）Android**继承扩展了Linux 内核安全模型的用户与权限机制。但通过应用程序沙盒隔离应用**，避免操作系统内存损坏;（2）Android **通过 AndroidManifest.xml 文件可以赋予应用额外的、细粒度的权限**；（3）与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——Binder，但与前者不同的是，Binder 机制更加灵活，可靠性更高**。它运行在单个设备上，不支持 RPC 网络远程调用；（4）Android 沿用了 Linux **安全增强技术 SELinux**。

**问答题**

**1、POSIX是IEEE为Linux定制的可移植操作系统接口，请简述POSIX的权能机制。**

要点：（1）**权能的含义**；（2）POSIX权能机制的**目的**；（3）**权能机制的含义**

参考答案：

权能是一种用于实现恰当特权的能力令牌。POSIX权能机制是一种基于权能的最小特权控制机制，其目的是实现比超级用户模式更细粒度的授权控制。它将特权划分成了一个权能集合。

POSIX权能机制提供了更为便利的权能管理和控制：一是提供了为系统进程指派一个权能去调用或执行受限系统服务的便捷方法；二是提供了一种使进程只能调用其执行特定任务必须权能的限制方法，支持最小特权安全策略的实现。它通过进程和程序文件权能状态(许可集、可继承集、有效权能集)，明确定义了进程如何获取和改变权能的语义，从而提供了一种基于进程所运行上下文控制进程权能的方法。

**2、如何保护文件加密密钥（FEK）？一旦用户删除或系统重装，Windows操作系统中的加密文件还能够恢复吗？**

**要点**：（1）用户口令保护用户的主密钥，而主密钥保护用户的私钥，用户的公钥加密FEK；（2）如果没有备份证书和私钥，无法恢复文件；（3）如果备份了证书和私钥，则可以恢复文件。

**第7章 数据库系统安全作业**

一、填空题

1、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

2、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） 。

3、数据库系统一般分为两个部分： 数据库 ， 数据库管理系统 。

4、数据库加密分为 库内 加密和 库外 加密。

5、安全审计的分析方法包括： 潜在违规分析 ， 基于异常检测的描述 ， 简单攻击试探法 ， 复杂攻击试探法 。

二、选择题

**1、以下描述是正确的是（ B ）**

A. 数据库在执行事务处理时，先操作数据库，再写日志；

B. 数据库在执行事务处理时，先写日志，再操作数据库；

C．数据库在执行事务处理时，只需要操作数据库，不需要写日志；

D. 数据库在执行事务处理时，操作数据库和写日志同时进行。

**2、用户访问数据库时，涉及以下哪些安全内容（ ABCE ）**

A. 授权规则；B. 语义完整性检查；C. 用户登录鉴别；D.数据加密；E. 审计追踪

**3、根据数据库的特点和实际需求，数据库加密必须满足以下要求（BCE）**

A.对数据库加密对原有系统功能的影响不大；

B.加解密的速度必须足够快，特别是对解密的速度要求更高；

C.加密机制在理论上和计算上都具有足够的安全性；

D.加密后的数据库存储量不增加，不能破坏字段长度的限制；

E.加解密对数据库的合法用户是透明的。

**4、数据库加密的粒度可以分为以下哪几类（ABCEF ）**

A.数据库；B.表；C.记录；D.页面；E.字段；F.数据项

三、简答题

**1. 数据库加密应具备哪些要求？**

要点：数据加密方法应在**保证安全**的前提下，首先考虑**加解密的效率**。因此，数据库加密方法选择需要注意以下几点：

1. 由于数据库中的记录保存时间相对较长，因此加密算法强度要求高。
2. 数据库加密以后，明密文数据长度相同或者相当，不应明显增加，避免数据库管理系统有较大变动。
3. 对于大型数据库系统而言，数据库最常见的使用方式是随机访问，所以加解密速度要足够快，对数据操作响应时间的影响应在用户可接受的范围内。
4. 加密算法应该能够直接对记录或者字段进行加密。

**2、操作系统安全威胁和数据库安全威胁分别是什么？为什么不同？**

要点：（1）**操作系统安全威胁只有软威胁，而数据库安全威胁不仅有软威胁，还有硬威胁、传输威胁、人为威胁和物理环境威胁**；（2）与OS不同，数据库安全威胁是指针对数据安全而言，主要影响数据安全的都可以称为数据库安全威胁；（3）OS不是没有物理安全威胁，而是统统划归物理安全中，这是因为，OS是安装在物理平台上的，硬件平台的安全就是OS的物理安全，所以不需要另外再描述。

四、问答题

**1. 什么是数据库系统的安全策略？它包括哪几个方面，目的分别是什么？**

要点：（1）安全策略是数据库系统组织、管理、保护和处理敏感信息的原则；（2）安全管理策略定义用户共享数据，并控制共享数据的使用；（3）信息流控制策略定义程序对数据的访问级别；（4）访问控制策略设定了不同角色对于数据库不同部分的访问权限。

参考答案：

数据库系统的安全策略是指导数据库系统安全的高级准则，即组织、管理、保护和处理敏感信息的原则，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，这种功能可由拥有者完成，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。不同的数据库根据其安全属性的敏感程度可以分为不同的安全级别。对于数据库系统的信息流控制，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。数据库系统的访问控制一般分为集中式控制和分布式控制两类。集中式控制系统只有一个授权者，他控制着整个数据库的安全。分布式控制系统是在一个数据库系统中有多个数据库管理员（DBA），每个管理员控制数据库的不同部分。

**2.数据库的恢复技术包含哪些，各有什么特点？**

要点：（1）事务故障恢复，利用日志Undo事务已经完成的那一部分修改；（2）系统故障恢复，Undo未完成的事务，Redo已经提交的事务；（3）介质故障的恢复，基于备份、副本，恢复数据。

**第8章 入侵检测技术作业**

**一、填空题**

1. 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。

2．入侵检测系统能够检测的入侵行为包括： 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 。

3. 审计数据的预处理方法包括： 数据集成 、 数据清洗 、 数据变换 、 数据简化 、 数据融合 。

4. 入侵信号的主要分析方法： 模式匹配 、 统计分析 、 完整性分析 。

**二、选择题**

1. 基于网络的入侵检测系统，需要把网卡设置成（D）

A. 单播模式；B. 广播模式；C. 多播模式；D.混杂模式

2. 基于主机的入侵检测系统，需要收集以下哪些信息（ACDE）

A. 系统日志；B. 网络日志； C.目录和文件中的异常改变；D.程序中的异常行为；E. 物理形式的入侵信息

3. 以下哪些内容是安全日志要记录的内容（ ABCD ）

A. 各种类型的登录日志；B. 对象的访问日志；C. 进程追踪日志； D. 特权使用日志；E. 目录或文件的修改日志。

4．入侵检测的主动响应行为包括（ ABC ）

A. 断开网络连接；B.杀死可疑程序；C.对攻击系统实施反击；D.增加审计日志；E.向管理员报警

**三、简答题**

**1. 入侵检测系统的优、缺点是什么？分析这些优、缺点给信息系统安全设计所带来的影响。**

参考答案：

（1）入侵检测的**优点**包括：**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**。

（2）但入侵检测也存在**缺点**，即：它**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；不能处理有关 package-level攻击**。

（3）给信息系统安全设计带来的**影响**是：**与其他安全技术**，如：防火墙、身份认证、访问控制、安全审计等**互补**，**但无法弥补这些系统本身的缺陷**；可以**为其他安全系统的完善提供有针对性的意见**。

**2.分析包捕获机制的作用和局限性。**

要点：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。

参考答案：

**作用**：（1）包捕获**为数据包捕获软件的设计提供了工作机制，作为sniffer、winpcap、wireshark、tcpdump等工具的底层原理提出**。（2）建立在目标系统上，**帮助实现网络数据包的实时获取、管理和控制**。

**BPF数据包捕获机制的局限性**：虽然过滤一部分数据包在一定的程度上降低了系统的开销，提高了效率。但它的**捕获和过滤都是在linux内核中完成。这样一来只要linux内核一更新，它也需要更新，降低了它的可移植性和通用性**。

**Libpcap数据包捕获机制的局限性**：数据包经过了linux得内核网络协议栈，从网卡到用户空间的传递过程，存在多次的拷贝和中断相应，**消耗大量的cpu时间片，降低系统整体的数据分析能力**。

**3. 安全日志和审计数据的区别？**

要点：（1）**审计数据的访问**比安全日志的**范围大**。（2）**安全日志记录的是安全审计事件**，如：各种类型的登录日志、对象访问日志、进程追踪日志、特权使用日志、账号管理日志、策略变更日志、系统事件日志等。（3）**审计数据不仅包含安全日志，还包含目录或文件的非法改动、网络流量数据或资源使用情况等**。

**四、问答题**

**1、举例说明基于协议分析的入侵检测系统。**

要点：（1）基于协议分析的入侵检测系统的特点；（2）举例说明这种IDS的工作原理。

注意：需要查阅资料

**2、在入侵检测系统中，如何获取直接监测数据？举例说明**

要点：（1）什么是直接监测数据获取。（2）举例说明，不仅限于系统资源使用情况的数据获取，如：获取CPU资源的使用情况

注意：需要查阅资料

第9章 可信计算作业

**一、填空题**

1、TCG可信计算的概念定义了哪些安全属性： 可鉴别性（或可认证性） 、 完整性 、 机密性 。

2、平台可信的起点是 TPM ；系统安全的起点是 可信根 ；静态信任度量的起点是 CTRM ；静态度量的可信根是 CTM ；

3、可信计算的基本功能： 完整性度量、存储和报告 ； 平台证明 ； 受保护能力 。

4、可信平台的可信根包括： RTM 、 RTS 、 RTR 。

5、TPM至少应该具备的4个功能是 对称/非对称加密 、 安全存储 、 完整性度量 和 签名认证 。

6、对PCR值修改的操作为： 重置 、 扩展 。

**二、选择题（包括单选和多选）**

1、可信是客观事实，而信任是主观评价。信任的基本属性包括：（**ACDE**）

A. 二重性；B. 对称性；C. 可度量性；D.可传递性；E. 动态

2、以下说法正确的是（**CDE**）

A. 可信计算平台只能运行可信应用；

B. 动态可信度量和静态可信度量的起点是相同的；

C. CRTM是静态可信度量的起点；

D. 信息系统启动的顺序会影响可信度量散列值；

E. 平台证明只用于远程调用；

F．TPM可以同时接收多条操作指令。

**三、简答题**

1、可信的概念？

要点：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。

2、实现可信计算时，需要达到哪些要求？

要点：（1）验证用户的身份；（2）验证平台软硬件配置的正确性；（3）验证应用程序的完整性和合法性；（4）平台之间的可验证性

答案：（1）验证用户的身份：验证使用者的合法身份，可以使用该系统；（2）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；（3）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；（4）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。

3、TPM至少应该具备的4个功能是什么？

要点：（1）对称/非对称加密；（2）安全存储（3）完整性度量（4）签名认证

**四、问答题**

**1. 静态度量时，可信平台的起点是 BIOS。它是否与 TPM 的目的有冲突，是否存在安全问题？分析说明。**

**要点：有冲突**，CRTM首先需要度量BIOS，把CRTM放在BIOS里面不符合TPM的目的。**安全问题：**（1）BIOS安全级别低于TPM芯片，易受恶意代码攻击；（2）BIOS对信息系统或TPM控制权过大，引发安全问题。

**参考答案：**TCG给出的信任链是CRTM→BIOS→OSLoader→OS→Applicatons，系统加电后需要由可信代码CRTM去度量BIOS代码的完整性。TPM的设计是基于可信的CRTM开始的信任链进行完整性度量，以此为起点保证整个平台的可信，因此最符合这一设计的方法是把CRTM嵌入TPM芯片内。如果起点在BIOS代码中，会导致BIOS自身代码的完整性没有经过度量，不符合TPM的目的。

存在的安全问题是，BIOS不具备TPM模块的安全级别，其中的代码有经受恶意代码攻击的风险。同时BIOS还需要完成硬件设备和配置信息的自检，具备对信息系统极大的控制权，以此作为可信平台的起点也构成安全问题。

**2.为什么要用 AIK 替代 EK？分析说明。**

**要点：**（1）EK与系统绑定，不能迁移；（2）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，保护用户隐私。

**参考答案：**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.详细分析基于静态可信根度量的缺陷。动态可信度量能够解决这些缺陷吗？为什么。**

**要点：（**1）静态可信根度量无法保证系统运行时安全；（2）可以抵御针对BIOS的攻击和BootLoader的漏洞，但是存在TPM重置攻击的风险；（3）DRTM没有解决软件可信的问题。

**参考答案：**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。

**4.SRK 是什么？其主要用途是什么？是否可以迁移？**

**要点：**（1）存储密钥根。管理用户数据，作为密钥树的根节点，保护子密钥。（2）不能，一个是部分子密钥不能迁移导致SRK不能迁移，另一个是SRK需要对持久存储区进行加密保护。

**参考答案：**SRK即存储根密钥，是存储密钥的一个特例。整个系统拥有一个最高权限的存储密钥，这个最高级密钥也就是存储根密钥。它很特殊，在每个用户创建的时候生成，管理这个用户的所有数据，也就是存储可信根。和背书密钥一样，一个TPM仅存在唯一一个。所有其它的密钥都在存储根密钥的保护之下。

由于SRK作为父密钥对子密钥进行加密保护，并配合密钥访问控制机制保证密钥体系安全，而在密钥树上的部分密钥是不可迁移的。此外，由于 TPM 的存储容量有限，因此一般在磁盘上还需要构建一个持久存储区，使用 SRK 进行加密保护，从而保证受保护的数据可以扩充。综合以上两点SRK不能迁移。

第10章 信息系统安全管理作业

一、填空题

1、信息系统安全管理的核心是 风险管理 。

2、信息系统安全管理的五要素分别为： 管理的主体（或主体） ， 管理的客体（或客体） ， 管理目标 ， 管理手段 ， 管理环境 。

3、信息系统安全管理分为 宏观管理 和 微观管理 。

4、信息系统安全的宏观管理属于 政府（或国家） 管理范畴，包括： 战略方针 ， 各项政策 ， 法律和法规 ， 标准 。

5、信息系统安全的微观管理属于 机构 管理范畴，包括： 策略 ， 规章 ，制度 ， 实践 。

6、信息系统安全管理中的PDCA模型分为 计划 、 实施 、 检查 、 处置 。

7、安全控制措施主要分三种类型： 管理控制 ， 技术控制 ， 物理控制 。

8、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。

二、选择题（包括单选和多选）

1、人员安全管理的原则是（**BCDEF**）

A．人员安全审查原则；B. 职责分离原则；C. 岗位轮换原则；D. 最小特权原则；E. 强制休假原则；F. 限幅级别

2、数据库备份时，写日志和写数据的顺序是（**B**）

A. 先写数据，再写日志； B. 先写日志，再写数据；C.日志和数据同时写；D. 日志可以不写。

3、以下表述是正确的（**ABC**）

A. 风险与生俱来，信息安全是相对的；

B. 信息系统安全管理体系是基于风险的信息安全管理体系；

C. 信息系统安全建设是在综合考虑成本和效益的前提下，制定控制风险的方法；

D. 信息系统安全管理的目的是消除风险。

三、简答题

1、什么是信息系统安全管理？

要点：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。

2、信息系统安全标准的重要性？

要点：（1）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；（2）信息系统安全标准是安全技术的制高点；（3）信息系统安全标准关系到国家的安全和利益。

3、我国信息安全管理存在的问题？

要点：（1）信息安全管理现状比较混乱，缺乏一个国家层面的整体策略；（2）信息系统安全管理体系还未建立起来；（3）信息系统安全风险评估标准体系还有待完善；（4）信息安全意识缺乏；（5）专项经费投入不足，管理人才缺乏；（6）技术创新不够；（7）缺乏权威、统一、专门的立法管理机构；（8）太多沿用国际标准。

4、如何理解信息系统安全管理中的分权和授权原则？举例说明

要点：（1）分权和授权是对特定职能或责任领域的管理功能实施分离、独立审计等分权，避免权力过分集中所带来的隐患；（2）例如（不一定是这个例子，但一定是安全方面的例子）：系统管理员和系统审计员的权限分属两个人。

5、人员安全管理包含哪些内容？

要点：安全组织建设；人员安全审查；安全培训和考核；签订安全保密合同； 离岗人员的安全管理；人员安全管理原则。

第11章 安全风险评估和等级保护

一、填空题

1、信息系统建设的起点和源头是 信息系统安全风险评估 。

2、信息系统安全风险分析涉及 资产 、 威胁 、 脆弱性 等三个基本要素。

3、评价资产的三个安全属性是 保密性 、 完整性 、 可用性 。

4、威胁的基本属性包括 威胁的主体 、 影响的对象（或威胁的对象） 、 动机 、 途径 。

5、信息系统基本安全需求包含 基本安全技术需求 和 基本管理需求 。

6、基本安全技术需求包含 物理安全 、 网络安全 、 系统安全 、 应用安全 和 数据安全 等5个层面。

7、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

二、选择题（包括单选和多选）

1、残余风险是由以下原因造成（ABC）

A. 安全措施不当造成的；

B. 安全措施失效造成的；

C．综合考虑了安全成本与效益后未去控制造成的；

D. 组织机构变化后，引入的风险。

2、以下安全措施属于预防性安全措施的有（ABD）

A. 防火墙；B. 入侵检测；C. 入侵容忍；D. 访问控制

3、以下说法正确的是（AB）

A. 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；

B. 根据威胁出现的频率和脆弱性的严重程度判断安全事件发生的可能性；

C. 根据资产的价值和脆弱性的严重程度判断安全事件发生的可能性；

D. 根据威胁出现的频率和资产的价值判断安全事件发生的可能性

4、以下说法正确的是（ABDE）

A. 脆弱性识别需要具体到每个资产或组件上；

B. 安全措施的确认不需要具体到每个资产或组件上；

C. 保护性安全措施可以降低安全事件发生的可能性；

D. 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；

E. 安全措施的实施是以减少脆弱性或降低安全事件发生的概率为目标的。

4、以下说法正确的是（AD）

A. 资产的重要性可以选择保密性、完整性和可用性上的任何一个赋值表示；

B. 资产的重要性只能综合考虑保密性、完整性和可用性上赋值；

C. 资产的重要性取决于资产的经济价值；

D. 资产的重要性取决于资产的价值。

5、以下哪种情况会出现欠保护（ B ）

A. 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；

B. 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；

C. 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；

D. 根据信息系统安全等级不同，采用不同的安全措施。

三、简答题

1、信息系统安全风险评估的概念？

要点：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。

2、在什么情况下进行信息系统安全风险评估？

要点：（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。

3、信息系统安全风险评估的可控性原则是什么？

要点：（1）服务可控性；（2）人员与信息可控性；（3）3）过程可控性；（4）工具可控性

4、什么情况下会造成残余风险？

要点：（1）信息系统的安全措施配置不当或失效；（2）综合考虑了安全成本与效益后未去控制造成的。

5、风险评估工具选择的原则？

要点：（1）实际需要原则；（2）试用原则；（3）实用原则；（4）满足脚本数量与更新速度要求；（5）支持不同级别的入侵检测

四．计算题

1、假设：某信息系统有3个重要的资产*A*1=2，*A*2=1，*A*3=3，，其中*A*1面临三个主要威胁*T*1=1，*T*2=5，*T*3=4；*A*2面临两个主要威胁*T*4=3，*T*5=4；*A*3面临两个主要威胁*T*6=3，*T*7=4。威胁*T*1可以利用资产*A*1存在的一个脆弱性*V*1=3；威胁T2可以利用资产*A*1存在的两个脆弱性*V*2=1，*V*3=5；威胁*T*3可以利用资产*A*1存在的一个脆弱性*V*4=4。威胁*T*4可以利用资产*A*2存在的一个脆弱性*V*5=4；威胁*T*5可以利用资产*A*2存在的一个脆弱性*V*6=3。威胁*T*6可以利用资产*A*3存在的一个脆弱性*V*7=2；威胁*T*7可以利用资产*A*3存在的一个脆弱性*V*8=3。

计算各资产在不同威胁和脆弱性下的风险值，判定各风险值的风险等级。

答题思路：

（1）安全事件发生概率的计算和安全事件发生后的损失计算可以采用公式