华文慕课操作系统与虚拟化安全课后作业答案 **-**生活小技巧

操作系统与虚拟化安全课后作业答案

**第1章计算机系统安全的重要性与评测标准**

**1、(5分)你知道下面哪些是开源的操作系统软件吗?** A、Linux

B、Android C、Windows D、iOS

答案 A,B

2、(13分)你知道下面哪些是开源的虚拟化软件吗？ A、KVM+Qemu

B、Xen

C、Hyper-V

D、VMWareWorkstation

答案 A,B

3、(13分)下面哪些是针对计算机系统的典型攻击模式？ A、拒绝服务

B、软件漏洞

C、恶意代码植入 D、人员错误

答案 A,C

4、(13分)下面哪些安全操作系统是通过认证达到了美国可信计算机系统评估准则(TCSEC)B2级以上的实际产品？

A、Multics操作系统

B、DTOS分布式可信微内核操作系统 C、TrustedXENIX操作系统

D、STOP基于安全通信处理器SCOMP的可信操作程序答案 C,D

5、(13分)信息安全领域内具有里程碑意义的彩虹系列中包括一个标准和一套体系，这个标准在发布时使用的纸质封皮是橘色的，也被称为橘皮书。请问，这个标准是哪个标准？

A、美国标准TCSEC(TrustedComputerSystemSecurityEvaluationCriteria) B、国际标准CC(CommonCriteria),即ISO/IEC15408

C、欧盟标准ITSEC(InformationTechnologySecurityEvaluationCriteria) D、美国联邦FC(FederalCriteriaforInformationTechnologySecurity)

答案 A

6、(13分)TCSEC和CC标准可以用于评估哪些计算机系统的可信级别或评估保证级别？ A、操作系统

B、数据库管理系统 C、网络组件

D、应用程序答案 A,B,C,D

7、(13分)TCSEC的可信等级划分包括D,C1，C2，B1，B2，B3,A四类七个等级。请问，从哪个级别开始要求实施强制访问控制？

A、自主级(C1,Discretionary)

B、受控访问级(C2,ControlledAccess)

C、结构化保护级(B2,StructuredProtection)

D、标记安全保护级(B1,LabeledSecurityProtection)

答案 D

8、(13分)CC标准中的TOE是评估对象，PP是安全保护轮廓，ST是安全目标。下面的描述正确的有哪些？

A、TOE是指作为评估主体的IT产品或系统，以及相关的指导性文档。

B、PP是指满足特定用户需求的、一类TOE的、一组与实现无关的安全要求。 C、ST是作为一个既定TOE的评估基础使用的一组安全要求和规范。

D、CC只考虑安全功能要求，不考虑安全保证要求。答案 A,B,C

第2章计算机系统基本安全概念和设计思想

1、(10分)访问控制思想涉及主体和客体的概念，操作系统中的主体通常指的是什么？ A、目录

B、进程 C、文件 D、用户答案 B,D

2、(13分)一个安全的计算机系统通常需要包括哪些安全需求？ A、机密性

B、完整性 C、可用性 D、可靠性答案 A,B,C

3、(13分)机密性是指要对数据的内容或者存在性保密，通常采取的保护机制是什么？ A、加密

B、记录与审计 C、检测与恢复 D、访问控制答案 A,D

4、(13分)计算机系统的安全性设计应该包括的三大要素是指什么？ A、安全保证

B、安全机制 C、安全策略 D、安全概念答案 A,B,C

5、(13分)基于UNIX的视窗系统X11提供了一种语言，以控制对控制台（用于X11显示视图的）的访问，如xhost+groucho–chico表达了一种安全策略，即允许来自主机groucho的连接请求，拒绝来自主机chico的连接请求，试问，这里采用的是高级策略描述语言吗？

答案：错误

6、(13分)安全内核的设计与实现应符合的基本原则有那些？ A、完整性原则

B、隔离性原则 C、可验证性原则

D、使用方便性原则答案 A,B,C

7、(13分)安全模型是安全策略的清晰表述，具有的主要特点包括哪些？ A、是简单的和具体的，易于实现

B、是精确的，无歧义的

C、是简单的和抽象的，易于理解

D、只涉及安全性质，不限制系统的功能与实现答案 B,C,D

8、(13分)计算机系统中负责实施安全策略的软件、硬件和人员等一起组成系统的可信计算基 (TrustedComputingBase,TCB)，下面哪些部分不属于操作系统的TCB？

A、操作系统的安全内核 B、具有特权的程序和命令

C、与安全策略配置相关的管理人员与文档 D、不涉及敏感信息访问的应用程序

答案 D

第3章访问控制机制

1、(13分)访问控制的主要任务是什么？ A、访问授权

B、访问决策 C、访问实施 D、访问需求答案 A,B,C

2、(5分)自主访问控制的自主性体主要现在哪些方面

A、一个用户可以自主地将他所拥有的资源授予其他用户访问

B、一个特定授权的用户（非所有者）能够自主地将访问权或访问权的某个子集授予其他用户

C、一个用户可以将他被授权访问的所有资源自主地授予其他用户访问 D、一个用户可以将他被授权访问的特定资源自主地授予其他用户访问答案 A,B

3、(13分)针对自主访问控制实现技术描述正确的有哪些？

A、Linux2.6以上版本系统支持Owner/Group/Others9bit位自主访问控制的实现模式 B、Linux2.6以上版本系统支持ACL访问控制列表的实现模式

C、Linux2.6以上版本系统支持一个用户X将其拥有的文件file1只授予Y用户写访问 D、Linux2.6以上版本系统支持一个用户X将其拥有的文件file2授予所有用户读访问答案 A,B,C,D

4、(13分)基于行的自主访问控制实现技术，是将访问控制列表信息与用户或主体的信息关联在一起，下面哪些属于基于行的自主访问控制实现技术？

A、能力表 B、前缀表

C、基于口令的访问控制机制 D、ACL模式

答案 A,B,C

5、(13分)在Linux2.6以上系统中，如果一个用户X要将其文件file的读的权限授予Y用户，Y用户与X

用户属于统一用户组group1，下面哪个操作是正确的？

A、chmodu+rfile B、chmod740file C、chmodg+rfile

D、setfacl–mu:Y:r,file

答案 B,C,D

6、(13分)木马是一段计算机程序，表面上在执行合法功能，实际上却完成了用户不曾料到的非法功能。受骗者是程序的用户，入侵者是这段程序的开发者。木马必须具有那些功能才能成功地入侵？

A、入侵者要写一段程序进行非法操作，其行为方式不会引起用户的怀疑 B、入侵者必须设计出某种策略诱使受骗者接受这段程序

C、入侵者必须使受骗者运行该程序

D、入侵者必须有某种手段回收由木马发作为他带来的利益

答案 A,B,C,D

7、(13分)多级安全定义了安全级由密级和范畴集合组成，假设主体A的安全级为

{topsecret:NATO，NUCLEAR，CRYPTO}，客体X的安全级为{secret:NATO，NUCLEAR}，客体Y的安全级为:{topsecret:NATO，CRYTPO}，请根据BLP简单安全规则和\*规则，判定A对X,Y的访问权限？

A、A允许读X，允许写Y B、A允许写X，允许读Y C、A允许写X，允许写Y D、A允许读X，允许读Y答案 D

8、(13分)客体重用的定义为：“包含一个或多个客体的存储介质(例如，页面，磁盘扇区，磁带)的主体的重新分配。通过标准系统机制，为新的主体重新分配时不应含有任何可用的残留数据 ”，残留数据主要会发生在下列哪些过程中？

A、文件或目录删除之后的物理块空间 B、文件系统格式化之后的物理块空间 C、重新分配的内存空间

D、重新分配的高速缓存空间答案 A,B,C,D

1、(10分)CC标准中的TOE是评估对象，PP是安全保护轮廓，ST是安全目标。下面的描述正确的有哪些？

A、TOE是指作为评估主体的IT产品或系统，以及相关的指导性文档

B、PP是指满足特定用户需求的、一类TOE的、一组与实现无关的安全要求。 C、ST是作为一个既定TOE的评估基础使用的一组安全要求和规范。

D、CC只考虑安全功能要求，不考虑安全保证要求。答案 A,B,C

2、(10分)vSphere是VMware公司推出一套服务器虚拟化解决方案，其目前的5.0版本已经通过认证达到了CC标准的哪个可信级别或评估保证级别？

A、EAL2+ B、EAL3+ C、EAL4+ D、EAL5+

答案 C

3、(10分)访问控制思想涉及主体和客体的概念，操作系统中的客体通常指的是什么？ A、文件

B、目录 C、进程 D、用户答案 A,B

4、(10分)一个安全的计算机系统通常需要包括哪些安全需求？ A、机密性

B、完整性 C、可用性 D、可靠性答案 A,B,C

5、(10分)机密性是指要对数据的内容或者存在性保密，通常采取的保护机制是什么？ A、加密

B、访问控制 C、记录与审计 D、检测与恢复答案 A,B

6、(10分)完整性是指对数据或资源的可信赖程度，它通常用于表述防止不当或未经授权的修改。完整性包括数据的完整性和来源的完整性，通常采取的保护机制是什么？

A、加密

B、记录与审计 C、访问控制 D、检测与恢复答案 B,C,D

7、(10分)安全模型是安全策略的清晰表述，下面哪一条不属于其主要特点？ A、是精确的，无歧义的

B、是简单的和抽象的，易于理解

C、只涉及安全性质，不限制系统的功能与实现 D、是简单的和具体的，易于实现

答案 D

8、(10分)计算机系统中负责实施安全策略的软件、硬件和人员等一起组成系统的可信计算基 (TrustedComputingBase,TCB)，下面哪些部分属于操作系统的TCB？

A、不涉及敏感信息访问的应用程序 B、操作系统的安全内核

C、具有特权的程序和命令

D、与安全策略配置相关的管理人员与文档答案 B,C,D

9、(10分)在操作系统实施强制访问控制时，需要控制的客体资源主要包括哪些类型？ A、文件和有名管道

B、消息队列、信号量集合和共享存储区 C、进程

D、目录

答案 A,B,C,D

10、(10分)客体重用的定义为：“包含一个或多个客体的存储介质(例如，页面，磁盘扇区，磁带)的主体的重新分配。通过标准系统机制，为新的主体重新分配时不应含有任何可用的残留数据 ”，残留数据主要会发生在下列哪些过程中？

A、文件或目录删除之后的物理块空间 B、文件系统格式化之后的物理块空间 C、重新分配的内存空间

D、重新分配的高速缓存空间答案 A,B,C,D

第4章可追究机制

1、(5分)可追踪机制主要包括哪些机制？可追踪机制主要包括哪些机制？ A、标识与鉴别

B、可信路径 C、安全审计

D、客体重用答案 A,B,C

2、(13分)系统中的用户标识必须满足那些条件？ A、系统中的用户标识是由用户自己确定的

B、系统中的两个用户可以使用同一个标识 C、系统中的用户标识必须满足唯一性

D、系统中的用户标识是不能被伪造的答案 C,D

3、(13分)基于口令的鉴别机制是一种常用技术，其实现时需要注意的事项包括哪些？ A、对口令进行加密存储和访问控制

B、对传输过程中的口令进行保护 C、对口令允许尝试的次数进行限制

D、对每一次口令的使用和修改进行审计答案 A,B,C,D

4、(13分)对用户建立可信路径的实现方法是，使用通用终端向核心发一个特殊信号，这个信号是不可信软件无法拦截、覆盖或伪造的，这个信号称为安全注意键 Linux系统中实现的安全注意键是那些键的组合？

A、Alt+SysRq+k B、Ctrl+Alt+Del

C、Ctrl+Shift+Space D、Alt+Ctrl+C

答案 A

5、(13分)安全审计的主要目的是检测和阻止那些行为？ A、非法用户对计算机系统的入侵行为

B、合法用户的误操作 C、管理员的权限滥用

D、系统的意外错误和故障答案 A,B,C

6、(13分)为了确保审计员获得有价值的审计记录，系统必须保证做到哪几点？

A、保证审计记录的完整性 B、审计所有必要的事件

C、保证审计追踪过程的完整性 D、审计用户非敏感数据的读写答案 A,B,C

7、(13分)审计事件主要分为主体审计事件和客体审计事件，在针对主体审计事件的记录中，通常需要包括哪些信息？

A、主体的当前安全级别 B、主体所属用户的标识

C、主体执行的当前事件（如：系统调用）及其结果（如成功或失败） D、主体的标识t

答案 A,B,C,D

8、(13分)安全审计在操作系统内核进行实现时，主要需要完成如下哪些工作？

A、在安全相关系统调用中实现内核级的审计点，负责判定审计条件和记录审计数据 B、实现一个内核级审计线程，负责监听循环缓存区是否写满，若写满，将其写入磁盘 C、实现内核级的统一循环缓存区，用于缓存系统实时产生的各种审计记录

D、实现审计相关的管理接口和管理命令，用于审计的开关、审计事件和参数的设置等答案 A,B,C,D

第5章连续保护机制（I）

1、(13分)在操作系统中，恰当特权通常代表的是什么能力？ A、执行特定受限/安全攸关操作的能力

B、超越自主访问控制策略的能力 C、超越强制访问控制策略的能力 D、执行日常操作的能力

答案 A,B,C

2、(13分)Linux系统参照POSIX标准定义了一组权能，下面哪个权能代表可以执行改变属主操作？ A、CAP\_SETUID

B、CAP\_DACWRITE C、CAP\_MACREAD

D、CAP\_OWNER

答案 D

3、(13分)在操作系统中实现最小特权管理，需要将超级用户的特权进行划分，并通常是分别分配给

4个不同的管理员，包括：安全管理员、安全操作员、审计员和网络管理员等。根据课程介绍，你认为系统安全策略的配置权限应该分给如下哪个管理员？

A、安全管理员 B、网络管理员 C、安全审计员 D、安全操作员答案 A

4、(13分)POSIX标准建议进程和程序文件的权能状态集合有三种，他们是什么？ A、Permitted许可集

B、Effective有效集

C、Inheritable可继承集 D、Bounding最大集 答案 A,B,C

5、(13分)操作系统的系统调用exec是以新的进程映像去代替原来的进程映像，也就是说，exec系统调用并没有创建新的进程，只是替换了原来进程上下文的内容，例如：进程的代码段、数据段、堆栈段被替换了。关于exec这种说法正确的本质原因是什么？

A、exec时,进程的真实用户标识不变 B、exec时,进程的PID保持不变

C、exec时,进程的有效用户标识不变 D、exec时,进程的权能状态不变

答案 B

6、(13分)Linux中实现的权能遗传算法主要是在exec调用一个程序的过程中完成，新的进程权能状态主要与下面哪些因素有关？

A、原进程的权能状态

B、被调用程序文件的权能状态

C、系统对所有进程限定的最大权能集 D、原进程的真实用户标识

答案 A,B,C

7、(13分)系统的完整性要求主要包括哪些方面？ A、残留数据的完整性

B、存储数据的完整性 C、传输数据的完整性 D、处理数据的完整性答案 B,C,D

8、(13分)传输过程中对数据的完整性进行保护有多种要求，其中要求由接收者TCB自己，无需来自源可信IT产品的任何帮助，即能恢复被破坏的数据为原始用户数据，这属于那种要求？

A、数据交换完整性检测 B、源数据交换恢复

C、目的数据交换恢复 D、基本回退

答案 C

第6章连续保护机制（II）

1、(5分)隐蔽通道主要会导致什么后果？ A、数据被泄露

B、数据被破坏 C、数据不可用 D、数据被丢失答案 A

2、(13分)关于隐蔽通道的描述，下面不正确的是哪个？

A、1973,Lampson首次定义隐蔽通道，即如果一个通信信道既不是设计用于通信的，也不是有意用于传递信息的，则称该通信信道是隐蔽的

B、TCSEC的隐蔽信道定义是指，允许进程以违反系统安全策略的方式传递信息的信道。

C、在实施了强制访问控制的多级安全操作系统中，特洛伊木马利用隐蔽通道能够将高安全级信息传送给低安全级进程(木马主人）。

D、在实施了强制访问控制的多级安全操作系统中，隐蔽通道是指利用系统设计的通信机制来传递信息的信道，如进程间通信机制：共享内存、消息队列、信号量等

答案 D

3、(13分)TCSEC从哪个级别开始要求对系统的隐蔽通道进行分析，CC标准又是从哪个级别开始要求的？

A、TCSECB1,CCEAL4 B、TCSECB2,CCEAL5 C、TCSECB2,CCEAL4 D、TCSECB3,CCEAL5

答案 B

4、(13分)判别隐蔽存储通道的公认标准是Kemmerer标准，其中必须满足如下哪些条件？ A、发送方和接收方进程能访问共享资源的同一属性。

B、发送方进程能改变该共享资源的状态。

C、接收方进程能察觉该共享资源的状态变化。 D、发送方与接收方进程之间有同步机制。

答案 A,B,C,D

5、(13分)80年代以后出现了系统的隐蔽通道分析方法，它们主要包括？ A、Goguen等人提出的无干扰法

B、Kemmerer等人提出的共享资源矩阵法 C、Tsai等人提出的带有语义分析的信息流法 D、Denning等人提出的句法信息流分析法答案 A,B,C

6、(13分)隐蔽通道分析可以在从抽象的安全模型到系统机器代码的任何一个层次上进行，共享资源矩阵法主要适用于在哪个层次进行隐蔽通道分析？

A、描述性顶层规范级 B、安全模型级

C、源代码级 D、机器代码级答案 A

7、(13分)Tsai等人提出的带有语义分析的信息流法，可以从源代码级标识隐蔽通道。试问，从源代码级标识隐蔽通道具有的明显优点有哪些？

A、能找出所有隐蔽存储通道（除了硬件导致的通道以外）

B、能找出放置审计代码、延迟和噪音的位置 C、能评估访问控制检查点是否设置得合适

D、能找出所有隐蔽通道（除了硬件导致的通道以外）答案 A,B,C

8、(13分)隐蔽通道标识后需要通过带宽计算来度量每个隐蔽通道的危害程度。下面哪些属于影响隐蔽通道带宽计算的主要因素？

A、噪音因素，即干扰进程对通信变量进行操作 B、编码因素，即好的编码方案可以提高信道带宽

C、原语因素，即是否使用了速度最快的系统调用来实现通信 D、延时因素，即干扰进程分享CPU时间导致通信速度下降答案 A,B,C,D

1、(10分)完整性是指对数据或资源的可信赖程度，它通常用于表述防止不当或未经授权的修改。完整性包括数据的完整性和来源的完整性，通常采取的保护机制是什么？

A、检测与恢复 B、访问控制 C、记录与审计 D、加密

答案 A,B,C

2、(10分)基于行的自主访问控制实现技术，是将访问控制列表信息与用户或主体的信息关联在一起，下面哪些属于基于行的自主访问控制实现技术？

A、基于口令的访问控制机制 B、能力表

C、前缀表 D、ACL模式答案 A,B,C

3、(10分)对强制访问控制的描述不正确的是什么？

A、由系统来判定拥有某安全属性的主体是否允许访问某客体，但是客体的拥有者可以不受此约束

B、以某个用户身份运行的进程不能改变该用户本身及该用户所拥有客体的安全属性，所以简单地通过允许其他用户来访问一个文件不会泄露文件的内容

C、为每个主体和客体赋予安全属性，但是这些属性不像自主访问控制属性那样可以随意改变。

D、可以阻止进程创建共享文件，避免利用这些共享文件将敏感信息传递给另一个进程答案 A

4、(10分)可追踪机制主要包括哪些机制？ A、标识与鉴别

B、安全审计 C、可信路径 D、客体重用答案 A,B,C

5、(10分)用户在登录、定义用户的安全属性或改变文件的安全级时，他必须确定自己是在与真实的安全内核通信，而不是与一个特洛伊木马打交道。为此，系统必须提供的机制是什么？

A、可信路径 B、标识与鉴别

C、强制访问控制 D、自主访问控制答案 A

6、(10分)最小特权原则主要是为了减少哪些危害行为？ A、管理员的误操作

B、特权程序被恶意利用 C、特权程序意外出错 D、管理员滥用特权

答案 A,B,C,D

7、(10分)在操作系统中，恰当特权通常代表的是什么能力？ A、执行特定受限/安全攸关操作的能力

B、超越自主访问控制策略的能力 C、超越强制访问控制策略的能力 D、执行日常操作的能力

答案 A,B,C

8、(10分)Linux中实现的权能遗传算法主要是在exec调用一个程序的过程中完成，新的进程权能状态主要与下面哪些因素有关？

A、被调用程序文件的权能状态 B、原进程的权能状态

C、系统对所有进程限定的最大权能集 D、原进程的真实用户标识

答案 A,B,C

9、(10分)根据收发双方利用的共享资源不同，隐蔽通道通常分为哪两种类型？ A、隐蔽定时通道

B、隐蔽存储通道 C、真实隐蔽通道 D、潜在隐蔽通道答案 A

10、(10分)Tsai等人提出的带有语义分析的信息流法，可以从源代码级标识隐蔽通道。试问，从源代码级标识隐蔽通道具有的明显优点有哪些？

A、能评估访问控制检查点是否设置得合适

B、能找出所有隐蔽存储通道（除了硬件导致的通道以外） C、能找出放置审计代码、延迟和噪音的位置

D、能找出所有隐蔽通道（除了硬件导致的通道以外）答案 A,B,C

第7章安全模型（I）

1、(5分)开发一个形式化安全模型需要满足那些基本要求？ A、完备性

B、正确性 C、一致性 D、简明性

答案 A,B,C,D

2、(13分)操作系统内核变量非常多，如果采用状态机模型来建立其安全模型，容易导致状态爆炸，所以状态机模型不适合用来建立操作系统的安全模型，你认为这种描述正确吗？

答案：错误

3、(13分)下面哪些安全模型可以用于保证系统的完整性？

A、BIBA模型 B、RBAC模型 C、DTE模型 D、BLP模型答案 A,B,C

4、(13分)如果说一个客体的完整性被破坏，通常是指在信息的传输路径中存在对该客体的不可靠信息流，这个不可靠的信息流可能的来源是什么？

A、来自低完整性主体 B、来自低完整性客体 C、来自高完整性主体 D、来自高完整性客体答案 A,B

5、(13分)BIBA模型包含了低水印策略、环策略和严格策略，它们的安全性如何？ A、BIBA环策略的安全性最低，BIBA低水印策略的安全性最高

B、BIBA低水印策略的安全性最低，BIBA严格策略安全性最高 C、BIBA低水印策略的安全性最高，BIBA严格策略安全性最低 D、BIBA环策略的安全性最低，BIBA严格策略的安全性最高答案 A

6、(13分)在Sandhu的RBAC96模型中，RBAC2模型主要增加了那些约束关系？ A、角色之间的继承关系。

B、角色的成员数限制。

C、角色之间的静态互斥关系。 D、角色之间的动态互斥关系。答案 B,C,D

7、(13分)根据中国墙模型，假定公司A、公司B属于同一个利益冲突类P；公司X、公司Y属于另外一个利益冲突类Q，如果某个用户u曾经读取了公司A的数据之后，试问：用户u能否继续读取公司B的数据？它可以继续读取公司X的数据吗？

A、不可以读取B的数据，可以读取X的数据 B、可以读取B的数据，可以读取X的数据

C、可以读取B的数据，不可以读取X的数据 D、不可以读取B的数据，不可以读取X的数据答案 A

8、(13分)在DTE安全策略中，需要根据安全目标制定域定义表(DomainDefinitionTable)和域交互表 (DomainInteractionTable)，其中用于描述主体动态域转换的是哪个？

A、域定义表 B、域交互表 C、两者都是 D、两者都不是答案 B

第8章安全体系结构

1、(13分)某种类型的安全体系结构是为理解或者其它目的而提出的，它是满足某个假设的需求集合的一个设计，显示了把一个通用体系应用于具体环境时的基本情况。这种安全体系结构属于哪种类型的安全体系结构？

A、抽象体系 B、逻辑体系 C、通用体系 D、特殊体系答案 B

2、(13分)下面哪些属于安全体系结构设计的基本原则？ A、从系统设计之初就考虑安全性

B、应尽量考虑未来的安全需求 C、实施安全控制的极小化和隔离 D、安全相关功能必须结构化

答案 A,B,C,D

3、(13分)GFAC广义访问控制框架的主要优点是将访问控制机制的哪两个部分进行了分离？ A、访问控制规则部分

B、访问控制信息部分 C、访问控制实施部分

D、访问控制决策部分答案 C,D

4、(13分)FLASK体系结构为解决多种需求之间的冲突，提供了两个策略独立的数据类型来标识客体，这两个数据类型是什么？

A、可变长字符串类型的安全上下文 B、具有固定长数值类型的安全标识 C、可变长字符串类型的安全标识

D、具有固定长数值类型的安全上下文答案 A,B

5、(13分)FLASK体系结构中的客体管理器（OM）主要需要为客户端提供访问哪些决策接口？ A、访问决策接口

B、标记决策接口

C、多实例化决策接口 D、策略变更决策接口答案 A,B,C

6、(13分)FLASK体系结构中的安全服务器（SS）主要需要提供哪些功能？ A、安全策略决策

B、保持SIDs和安全上下文之间的映射

C、为新创建的客体提供SIDs（SecurityIdentifier） D、选项都不是

答案 A,B,C

7、(13分)LSM以内核补丁的形式实现，下面哪些方面是LSM对内核的修改？ A、新增安全系统调用

B、新增钩子函数的调用

C、在关键内核数据结构中新增安全字段 D、新增安全模块管理

答案 A,B,C,D

8、(13分)按照功能来分的话，LSM的钩子函数可以分为以下哪几类？ A、进行访问权限检查的钩子函数

B、在创建或者释放新的内核对象时同时创建或者释放安全字段的钩子函数 C、内核对象改变后，用来改变相应安全字段的钩子函数

D、选项全不对答案 A,B,C

第9章可信计算技术（访谈卿斯汉教授、王绍斌博士）

1、(5分)TCPA/TCG可信工作组定义了可信计算的属性，它们包括下面哪几个属性？ A、身份认证：计算机系统的用户可以确定与他们通信的对象身份

B、完整性：用户确保信息能被正确传输

C、私密性：用户相信系统能够保证信息的私密性

D、可靠性：用户可在任何需要服务的时刻即时得到服务答案 A,B,C

2、(13分)可信平台模块TPM的主要设计原则，除了需要考虑安全性、私密性原则之外，还需要包括哪些设计原则？

A、可互操作性原则 B、易用性原则

C、数据可移植性原则 D、可控性原则

答案 A,B,C,D

3、(13分)可信平台模块TPM至少提供如下哪些功能？ A、安全存储

B、签名认证 C、加密

D、完整性度量答案 A,B,C,D

4、(13分)可信计算平台模块管理的公私钥对有很多种，其中哪个公私钥是TPM的唯一标识，它永久性保存在TPM内部，并且禁止在外部使用？

A、SRK,StorageRootKey B、EK,EndorsementKey

C、AIK,AttestationIdentityKey

D、SRK和EK

答案 B

5、(13分)与可信平台模块相关的信任状主要包括哪些？

A、认可/背书信任状，颁发者证明对应EK的一个TPM是它们生产的

B、证实标识信任状，颁发者证明带有对应AIK的平台经证明已确认是一个可信平台 C、平台信任状，颁发者证明具有某特性的平台是它们生产的

D、一致性信任状，颁发者证明具有特定TPM的某可信平台符合TCG的相关标准/规范答案 A,B,C,D

6、(13分)可信平台模块提供的可信根有三种，他们指的哪三种？

A、可信存储根（RTS），提供密码机制保护存储在TPM之外的信息（数据和密钥） B、可信度量根（RTM），由平台提供的可对平台状态进行度量的机制

C、可信报告根（RTR），提供密码机制对TPM状态及信息进行签名 D、可信构造块（TBB），提供RTM和TPM初始化的信息和功能

答案 A,B,C

7、(13分)可信平台模块TPM1.1的身份认证采取的是PrivacyCA认证方案，其基础理论依据是什么？TPM1.2的身份认证采取的是DAA直接匿名认证方案，其基础理论依据又是什么？

A、一次一密和零知识证明，群签名 B、群签名和零知识证明，一次一密 C、群签名，一次一密和零知识证明 D、一次一密，群签名和零知识证明答案 D

8、(13分)与TPM1.2规范相比，TPM2.0规范的重要改进主要体现在那些方面？ A、提供了支持更多加解密算法的接口

B、清理了TPM设计，使其更简单、更便宜、更强壮和更易用等

C、增加了灵活性，支持更多的应用场景、使TPM变得更易用和可管理等 D、增加了一个安全/半安全时钟，与TPM1.2中的计数器相比更便宜

答案 A,B,C,D

1、(10分)开发一个形式化安全模型需要满足那些基本要求？ A、完备性

B、正确性 C、一致性 D、简明性

答案 A,B,C,D

2、(10分)操作系统内核变量非常多，如果采用状态机模型来建立其安全模型，容易导致状态爆炸，所以状态机模型不适合用来建立操作系统的安全模型，你认为这种描述正确吗？

答案：错误

3、(10分)在Sandhu的RBAC96模型中，RBAC2模型主要增加了那些约束关系？ A、角色的成员数限制。

B、角色之间的静态互斥关系 C、角色之间的动态互斥关系。 D、角色之间的继承关系。

答案 A,B,C

4、(10分)安全体系结构描述的是一个系统如何组织成一个整体以满足既定的什么要求？ A、性能要求

B、安全性要求 C、可扩展性要求 D、成本要求

答案 B

5、(10分)某种类型的安全体系结构是为理解或者其它目的而提出的，它是满足某个假设的需求集合的一个设计，显示了把一个通用体系应用于具体环境时的基本情况。这种安全体系结构属于哪种类型的安全体系结构？

A、特殊体系 B、通用体系 C、抽象体系 D、逻辑体系答案 D

6、(10分)Spencer等人提出的FLASK体系结构认为对策略灵活性的支持应该包括哪些内容？ A、支持多种安全策略

B、可实现细粒度的访问控制

C、能够确保访问权限的授予与安全策略保持一致 D、能够撤回先前已授予的访问权限

答案 A,B,C,D

7、(10分)FLASK体系结构为解决多种需求之间的冲突，提供了两个策略独立的数据类型来标识客体，这两个数据类型是什么？

A、可变长字符串类型的安全标识 B、可变长字符串类型的安全上下文 C、具有固定长数值类型的安全标识

D、具有固定长数值类型的安全上下文答案 B,C

8、(10分)FLASK体系结构中的安全服务器（SS）主要需要提供哪些功能？ A、安全策略决策

B、保持SIDs和安全上下文之间的映射

C、为新创建的客体提供SIDs（SecurityIdentifier） D、三项都不是

答案 A,B,C

9、(10分)可信平台模块TPM的主要设计原则，除了需要考虑安全性、私密性原则之外，还需要包括哪些设计原则？

A、可控性原则 B、易用性原则

C、可互操作性原则 D、数据可移植性原则答案 A,B,C,D

10、(10分)可信平台模块提供的可信根有三种，他们指的哪三种？

A、可信存储根（RTS），提供密码机制保护存储在TPM之外的信息（数据和密钥） B、可信度量根（RTM），由平台提供的可对平台状态进行度量的机制

C、可信报告根（RTR），提供密码机制对TPM状态及信息进行签名 D、可信构造块（TBB），提供RTM和TPM初始化的信息和功能

答案 A,B,C

第10章安全操作系统的设计与实现技术案例（访谈卿斯汉教授）

1、(5分)J.H.Saltzer在1975年提出安全系统八大设计原则，试问下面哪些原则不在其中？ A、基于“禁止”的安全

B、机制经济性

C、完全的访问仲裁 D、最小特权

答案 A

2、(13分)安全系统开发过程中进行的脆弱性评定通常需要包括哪些工作？ A、隐蔽通道存在性分析

B、可信计算基TCB的误用或不正确设置的可能性 C、攻破系统的概率或排列机制的可能性

D、可信计算基TCB的开发和操作中引入可利用脆弱性的可能性答案 A,B,C,D

3、(13分)安全系统开发过程中如果安全性与性能、兼容性发生矛盾，三者权衡顺序应该是？ A、安全性、兼容性、性能

B、安全性、性能、兼容性 C、兼容性、安全性、性能 D、兼容性、性能、安全性答案 A

4、(13分)符合中国GB17859-1999的安胜安全操作系统主要建立了哪几个形式化安全模型？ A、一种改进的可动态调节的机密性安全模型

B、基于DTE技术的完整性保护形式安全模型

C、支持POSIX权能的最小特权控制形式化安全模型 D、面向隐蔽存储通道分析的回溯搜索法

答案 A,B,C

5、(13分)基于DTE技术的完整性保护形式安全模型中引入了那些新的概念/关系？ A、可信管道与良构事务的分配关系

B、域之间的不可控制关系

C、可信管道与角色的分配关系 D、良构事务与角色的分配关系答案 A,B,C

6、(13分)支持POSIX权能的最小特权控制形式化安全模型中主要提出了管理层、功能控制层和应用层的层次化控制原则，它主要结合了那些策略和机制的设计思想？

A、RBAC基于角色的访问控制模型 B、TE基于型的强制实施策略

C、POSIX权能机制

D、ChineseWall中国墙模型答案 A,B,C

7、(13分)Kuhnhauser指出，一个灵活支持多策略的安全体系结构需要解决的主要问题有哪些？ A、策略实施

B、策略重用 C、策略冲突 D、策略协作答案 A,B,C,D

8、(13分)回溯搜索法主要适用于系统开发过程中哪个层次的隐蔽通道分析？ A、安全模型级

B、描述性顶层规范级 C、源代码级

D、形式化顶层规范级答案 C

第11章基于安全操作系统的应用-数据库安全（张敏老师的专题）

1、(10分)在如下各安全特性中，早期的多级安全数据库管理系统设计偏重于？ A、机密性

B、完整性 C、可用性

D、不可否认性答案 A

2、(20分)不属于多级安全数据库管理系统研究范畴的是？ A、数据库水印

B、多级数据模型 C、隐通道分析 D、数据库审计答案 A

3、(20分)B2级以上高等级DBMS多采用以下哪些体系结构？ A、可信主体

B、可信时间戳 C、集中式

D、复制式答案 C,D

4、(20分)下面属于外包数据库安全研究范畴的是： A、密文检索

B、查询完整性验证 C、数据库水印

D、SQL注入攻击及防范答案 A,B,C

5、(20分)在以下各类区间密文检索方案中，效率与可用性最好的是： A、保序加密

B、二次查询方案 C、加密B+树索引 D、加密B树索引答案 A

第12章系统虚拟化安全与虚拟可信平台技术

1、(5分)数据中心的系统虚拟化技术主要分为那几种？ A、PC/服务器虚拟化

B、桌面虚拟化 C、网络虚拟化

D、存储虚拟化答案 A,B

2、(13分)虚拟机监控器的实现方法主要包括哪几种？ A、泛虚拟化

B、全虚拟化

C、硬件辅助虚拟化

D、独立监控型/宿主型虚拟化答案 A,B,C

3、(13分)虚拟化计算平台的安全性需要通过多个方面的安全保障，主要包括哪些方面？ A、虚拟机监控器的安全保障

B、虚拟机的安全迁移

C、虚拟机状态的安全监控

D、虚拟机之间的隐蔽通道分析答案 A,B,C,D

4、(13分)Xen安全框架XSM设计目标是支持多种使用模型，主要包括哪几种使用模型？ A、用于分解Dom0（特权域）

B、用于划分资源

C、用于保护平台免受第三方软件攻击 D、用于保护平台核心的安全服务

答案 A,B,C,D

5、(13分)对虚拟机迁移请求进行安全决策过程中主要需要考虑哪些要素？ A、虚拟机源物理平台的完整性

B、虚拟机目标物理平台的完整性 C、虚拟机自身的完整性

D、虚拟机迁移请求者身份的真实性答案 A,B,C

6、(13分)XenAccess是一个安全灵活的虚拟机监控架构，为第三方安全监控软件提供了一整套的安 AP，可以使用户对虚拟机的那些资源操作进行监控？

A、网络

B、I/O C、磁盘 D、内存

答案 C,D

7、(13分)目前人们发现了一些虚拟机之间的隐蔽通道，下面哪些是属于隐蔽存储通道？ A、基于CPU负载的隐蔽通道

B、基于共享内存/Cache的隐蔽通道 C、基于mfn2pfn映射表的隐蔽通道 D、其他选项均不是

答案 C

8、(13分)虚拟可信平台技术中，选用生成EK证书的解决方案是实现虚拟TPM实例信任链扩展的关键，如果要求虚拟TPM和硬件TPM之间存在强连接，应该采取其中的那一种实施方案？

A、通过一个本地CA为虚拟TPM实例的EK发布证书，不与硬件TPM的证书建立证书链。 B、构建“发给一个虚拟TPM实例的EK证书”到“发给硬件TPM的AIK证书”的证书链。

C、不使用虚拟EK证书，而是根据为硬件TPM发布的AIK为虚拟TPM实例发布AIK证书。 D、其他选项方案均不可取

答案 B,C