第五章

一、填空题（分，每空 1 分）

2.访问控制是对主体访问客体的能力或权力的限制，它包括：**主体**、**客体**、**引用监控器**和**访问控制策略**四个要素。

3.访问控制的二元组描述方法通常包含**访问控制矩阵**、**访问控制表**、**访问能力表**和**授权关系表**四种形式。

4.基于所有权的访问控制分为：**自主访问控制**和**强制访问控制**。

5.访问控制实现的类别包括：**接入访问控制**、**资源访问控制**和**网络端口和节点访问控制**。

6.强制访问控制两种常见模型为：**BLP 模型**和 **Biba 模型**。

7.基于角色的访问控制模型族中包括 **RBAC0**、**RBAC1**、**RBAC2** 和 **RBAC3** 四个模型。

8.基于属性的访问控制模型以**属性**为最小的授权单位，替代基于角色的访问控制模型中以**身份标识**为依据的授权方式。

9.基于属性的模型中主要涉及四类实体属性：**主体属性**、**客体属性**、**环境属性**和**权限属性**。

二、选择题（22.5 分，每题 1.5 分）

1. 访问控制是指确定（A）以及限制主体访问客体的能力或权利。

A. 用户权限　　B. 可给予哪些主体访问权利

C. 可被用户访问的资源　D. 系统是否遭受入侵

2. 下列对访问控制影响不大的是（D）。

A. 主体身份　　B. 客体身份

C. 访问类型　　D. 主体与客体的类型

3. 下列关于访问控制主体和客体的说法中，错误的是（BD）

A. 主体是一个主动的实体，它提供对客体中的对象或数据的访问要求

B. 主体可以是访问信息的用户、程序和进程

C. 客体是含有被访问信息的被动实体

D.一个对象或数据如果是主体，则其不可能是客体

4. 为了简化管理，通常对访问者（A），以避免访问控制表过于庞大。

A. 分类组织成组　　B. 严格限制数量

C. 按访问时间排序，删除长期没有访问的用户

D. 不作任何限制。

5. 以下有关访问控制矩阵中行和列描述正确的是（B）

A. 行中放用户名，列中放对象名；

B. 行中放程序名，列中放用户名；

C. 列中放对象名，行中放设备名；

D. 列中放标题，行中放程序。

6. 以下对访问控制表和访问能力表说法正确的是（D）

A.访问能力表表示每个客体可以被访问的主体及其权限；

B.访问控制表说明了每个主体可以访问的客体及其权限；

C.访问控制表一般随主体一起保存；

D.访问能力表更容易实现访问权限的传递，单回收访问权限较困难。

7. 对类成员访问权限的控制，是通过设置成员的访问控制属性实现的，下列不是访问控制属性的是(D)。

A．公有类型　　B．私有类型

C．保护类型　　D．友元类型

8. 以下哪组都是完整性模型（B）

A.BLP 模型和 BIBA 模型　　B.BIBA 模型和 Clark-Wilson 模型

C.Chinese-wall 模型和 BLP 模型　　D.Clark-Wilson 模型和 BLP 模型

9.下面哪类访问控制模型是基于安全标签实现的？（B）

A．自主访问控制　　B．强制访问控制

C．基于角色的访问控制　　D．基于属性的访问控制

10. BLP 访问控制模型的读写原则是（A）

A.向下读，向上写　　B.向上读，向上写

C.向下读，向下写　　D.向上读，向下写

11. BIBA 访问控制模型的读写原则是（D）

A. 向下读，向上写　　B. 向上读，向上写

C. 向下读，向下写　　D. 向上读，向下写

12. 哪种访问控制技术适应于权限的频繁更改（C）

A. 自主访问控制　　B. 强制访问控制

C. 基于角色的访问控制　　D. 基于属性的访问控制

13. 在复杂架构的企业和机构中最适合的访问控制机制是（C）

A. 自主访问控制　　B. 强制访问控制

C. 基于角色的访问控制　　D. 基于任务的访问控制

14. 适合分布式计算和多点访问控制的信息处理的访问控制机制是（D）

A. 自主访问控制　　B. 强制访问控制

C. 基于角色的访问控制　　D. 基于任务的访问控制

15. 满足开放网络环境下资源访问控制要求的访问控制机制是（D）

A. 自主访问控制　　B. 基于属性的访问控制

C. 基于角色的访问控制　　D. 基于任务的访问控制

16. 下图为访问控制列表。以下说法正确的是（D）

主体	客体			
	File1	File2	File3	File4
N1	Own,R,W,E		Own,R,W,E	
N2	R	Own,R,W,E	W	R
N3	R,W	R		Own,R,W,E

A. N1 是管理员；　B. N2 是管理员；　C. N3 是管理员；　D. 都不是管理员

三、多选题（15 分，每题 3 分）

1. 安全系统在实现引用验证机制时必须同时满足以下哪些原则（A，C，D，E）

A.　必须具有自我保护能力；

B. 尽可能处于活跃状态，从而保证程序对资源的引用最大限度地得到引用验证机制的仲裁；

C. 防篡改，保持自身的完整性；

D. 不可绕过性；

E .必须设计得足够小，以利于分析和测试，从而能够证明它的实现是正确的

和符合要求的。

2. 访问控制策略的制定必须体现主体、客体和访问规则集等三者之间的关系，需要遵循以下原则（BCD）

A. 保密性原则 B. 最小特权原则 C.最小泄漏原则 D.多级安全原则

3. 有关访问控制列表（ACL）描述不正确的是（BCD）

A.表述直观，比较容易查出对某一特定资源拥有访问权限的所有用户；

B.单纯使用 ACL 可以实现复杂的安全政策；

C.单纯使用 ACL 可以实现最小权限原则；

D.对于较大规模的信息系统实现整个组织范围内一致的控制政策比较方便。

4. 下面哪些是 BLP 模型的主要任务：（ABC）

A.定义使系统获得“安全”的状态集合；

B.检查所有状态的变化均始于一个“安全状态”并终止于另一个“安全状态”；

C.检查系统的初始状态是否为“安全状态”；

D.选择系统的终止状态。

5. 关于访问控制列表和访问能力表的描述正确的是（ABC）

A. 对于访问权限浏览，访问控制表比访问能力表容易

B. 访问控制能力表比访问控制列表容易实现访问权限传递；

C. 访问控制列表比访问能力表容易实现访问权限回收

D. 访问控制列表转换到访问能力表比较难，而反之则相对容易；

四、简单题（25 分，每题 5 分）（见课后习题答案）

1、名称解释访问控制

A.得分点

（1）定义 1 分；（2）四要素。各 1 分；

B.参考答案

访问控制是对主体访问客体的能力或权力的限制，它包括四个要素：主体，客体，引用监控器和访问控制策略。

2、名称解释 自主访问控制，强制访问控制

A.得分点：

（1）自主访问控制 2.5 分 （2）强制访问控制 2.5 分

B 参考答案

答：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。（2.5 分）

强制访问控制，它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，即使是创建者用户，在创建一个资源后，也可能无权访问该资源。（2.5 分）

3、名称解释 基于角色的访问控制

A. 得分点

内容不完整扣 3 分；

B. 参考答案

基于角色的访问控制：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。

4、基于任务的访问控制

A.得分点

内容不完整扣 3 分；

B.参考答案

基于任务的访问控制（TBAC）采用“面向任务”的观点，从任务（活动）的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，因此，它是一种主动访问控制模型。

5、基于属性的访问控制

A.得分点

内容不完整扣 3 分；

B.参考答案

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。ABAC 模型以属性为最小的授权单位，替代基于角色的访问控制模型中以身份标识为依据的授权方式，以满足开放网络环境下资源访问控制的要求。

6、学校教务系统中，学生只有提交了评教，才能看到分数，这是“访问控制”吗？为什么？

参考答案：（1）是。（2）解释什么是访问控制；（3）这是访问控制策略，给出了主体访问课题的约束。

7、登录系统时的身份认证是接入访问控制吗？

参考答案：（1）不是。（2）解释什么是接入访问控制；（3）登录时的身份认证只是验证了用户身份的合法性，与访问哪些资源的权限无关。（4）之所以每个登录用户都具有某些资源的访问能力，是因为每个用户与用户的权限绑定在了一起。

五、问答题（30 分，每题 10 分）（见课后习题答案）

1、访问控制策略制定遵循的基本原则是什么？举例说明。

A.得分点

（1）遵循最小特权、最小泄漏、多级安全原则。每个原则 2 分

（2）举例的要求：最小特权应强调权限的最小划分，以保证对主体权力最大限度的限制，同时又不影响主体的功能实现；最小信息泄漏需要说明只有必要的信息被主体知道，是在主体确定做某件事之前把信息分配给主体；多级安全原则强调安全等级的划分，并基于安全等级限制信息的流动。4 分

B.参考答案

访问控制策略的制定必须体现主体、客体和访问规则集等三者之间的关系，遵循的原则如下：最小特权原则。在主体执行操作时，按照主体所需权力的最小化原则分配给主体权力。其优点是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，即为了达到一定目的，主体必须执行一定操作，但只能做被允许的操作。最小泄漏原则。主体执行任务时，按其所需知道的最小信息分配主体权限，防止信息泄密。多级安全原则。根据主体和客体之间流动的数据安全级别，将主、客体划分成 5 个安全等级：绝密（TS），秘密（S），机密（C），限制（RS）和无级别（U）。信息不允许从高安全级别向低安全级别流动，具有安全级别的信息资源，只有高于安全级别的主体才可访问，这样可以避免敏感信息扩散。

最小特权原则体现于惠普的 Praesidium/Virtual Vault。它通过以最小特权机制将根功能分成 42 种独立的特权，仅赋予每一应用程序正常运行所需的最小特权。因而，即便一名黑客将 Trojan Horse(特洛伊木马)程序安装在金融机构的 Web 服务器上，入侵者也无法改变网络配置或安装文件系统。最小特权是在惠普可信赖操作系统 Virtual Vault 的基本特性。

最小信息泄漏原则体现在面向对象的安全体系设计过程中。第二章提到的 CORBA 安全服务规范，各层次只将其他层次或模块需要的最小的信息对外开放，这些信息恰好能保证系统的正常运作。

Linux 等多用户的操作系统访问控制中应用到了多级安全策略。以 root 用户作为最高的安全级别，按照不同的安全级别可配置不同的用户组，以此来管理不同访问权限的文件和应用程序。

2、BLP 模型和 Biba 模型的安全策略和安全访问规则？分析它们的适用范围和可能存在的问题。

A.得分点

（1）BLP 模型采用多级安全的策略，访问规则包括强制安全访问规则和自主安全访问规则。2 分

（2）Biba 模型采用多级安全原则和最小泄漏原则。采用了五种非自主安全访问规则和基于 ACL、客体层次结构、环的自主安全访问原则。3 分

（3）BLP 模型中信息单向不可逆，客体具备高度机密，但是会带来隐藏通道问题。不能阻止未授权主体修改客体。3 分

（4）Biba 是完整性模型，能够于 BLP 模型结合。但是完整性级别标签确定困难、目的性不明确、与 BLP 结合困难。2 分

B.参考答案

BLP 模型的目的是保护数据的机密性，它将客体的安全级别分为绝密、机密、秘密和公开等四类。该模型详细说明计算机系统的多级操作规则，对应军事类型的安全级别分类，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

1）安全访问规则。BLP 模型的安全访问规则包括两类：强制安全访问规则和自主安全访问规则。强制安全访问规则包括简单安全规则和*策略，系统对所有的主体和客体都分配一个访问类属性，它包括主体和客体的密级和范围，系统通过比较主体与客体访问类属性来控制主体对客体的访问。自主安全访问规则使用一个访问矩阵来表示，主体只能按照矩阵中授予的访问权限对客体进行相应的访问。安全访问规则可以用三元组（s，o，m）表示主体 s 能够以权限 m 访问客体 o；$m=M(s, o)$ 表示主体 s 能够以权限 m 访问客体 o，其中 M 为访问矩阵；f 是主体或客体的安全级别函数，其定义为 $f: s \cup o \rightarrow L$，其中 L 为安全级别的集合。

规则 1：简单安全规则（Simple Security Property）如果主体 s 对客体 o 有读（Read）权限，则前者的安全级别不低于后者的安全识别。这一规则的形式化表示为

$$Read \in M(s, o) \Rightarrow (f\ s) \geqslant (f\ o)$$

这被称为“下读”原则。

规则 2：*策略（Star Property）

如果一个主体 s 对客体 o 有追加记录（Append）权限，则后者的安全级别一定不低于前者；如果主体 s 对客体 o 有读写（Read-Write）权限，则它们的安全级别一定相等；如果主体 s 对客体 o 有读（Read）权限，则后者的安全级别一定不高于前者。这一规则的形式化表示为

$$Append \in M(s, o) \Rightarrow (f\ s) \leqslant (f\ o)$$

$$Read\ and\ Write \in M(s, o) \Rightarrow (f\ s) = (f\ o)$$

$$Read \in M(s, o) \Rightarrow (f\ s) \geqslant (f\ o)$$

这被称为“上写”原则。

规则 3：自主安全访问规则

当前正在执行的访问权限必须存在于访问矩阵 M 中。这个规则保证主体 s 对客体 o 的权限是通过自主授权来进行的。这一规则的形式化表示为

$$(s, o, m) \in b \Rightarrow m \in M(s, o)$$

其中，b 表示在某个特定状态下，哪些主体以何种访问属性访问哪些客体的一个集合上述规则保证了客体的高度机密性，保证了系统中信息的流向是单向不可逆的，即信息总是从低密级的主体向高密级的主体流动，避免敏感信息的泄露。同时，利用 BLP 模型可以分析同一台计算机上并行运行不同密级的数据处理程序的安全性问题，可以检验高密级处理程序是否把敏感数据泄漏给了低密级处理程序，或低密级处理程序是否访问了高密级数据。

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（Critical，C），非常重要（Very Important，VI）和重要（Important，I），它们的关系为 C＞VI＞I。在 Biba 模型中，主要访问方式有四种：修改（modify），调用（invoke），观察（observe）和执行（execute）。与 BLP 类似，Biba 模型的访问规则也分为两类：非自主安全访问规则和自主安全访问规则。

非自主安全访问规则。非自主安全访问规则是基于主体和客体各自的完整性级别，确定主体对客体的访问方式。Biba 模型中有五种非自主安全访问规则：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。

自主安全访问规则。Biba 模型中的自主安全访问规则用到了如下访问策略：1）访问控制列表（Access Control List）对每个客体分配一个访问控制列表，指明能够访问该客体的主体，以及主体访问该客体的方式。但客体的访问控制列表可以被对该客体拥有 modify 访问权限的

主体修改。

2）客体层次结构（Object Hierarchy）模型将客体组织成树状结构，一个客体的中间节点是从此客体节点到根的路径上的所有节点。如果一个主体要访问一个客体 ，则必须对此客体的所有中间节点拥有 observe 权限。

3）环（Ring）对每个主体分配一个权限属性，称为“环”。环用数字表示，数字越低，权限越高。

自主安全访问规则基于以下要求：

一个主体仅在环允许的范围内对客体拥有 modify 访问方式。

一个主体仅在环允许的范围内拥有对另一个具有更高权限的主体的 invoke 访问方式。

一个主体仅在环允许的范围内对客体拥有 observe 访问方式。

Biba 模型是一个完整性模型，但却是一个与 BLP 模型完全相反的模型，一旦将保密性和完整性同时考虑时，必须注意不要混淆保密性访问和完整性访问，它们两个是相互独立的，之间没有任何关系。Biba 模型的优势在于其简单性以及与 BLP 模型相结合的可能性，但也存在以下方面的缺陷：完整性级别的标签确定困难。由于 Biba 模型的机密性策略与政府分级机制完美结合，所以很容易确定机密性标签的分级和范围，但对于完整性的分级和分类一直没有相应的标准支持。Biba 模型的目的性不明确。Biba 模型保护数据免受非授权用户的恶意修改，同时认为内部完整性威胁应该通过程序验证来解决，但在该模型中没有包含这个要求，因此，Biba 模型在保护数据一致性方面不充分。Biba 模型与 BLP 模型结合困难。虽然这种实现机密性和完整性的方法在原理上是简单的，但是由于许多应用内在的复杂性，使得人们不得不通过设置更多的范围来满足这些复杂应用在机密性和完整性方面的要求，这些不同性质的范围在同时满足机密性和完整性目标方面是很难配合使用的，很容易出现进程不能访问任何数据的局面。同时，Fred Cohen 已经证明即使使用了 BLP 模型和 Biba 模型，也无法抵御病毒的攻击

3、如何理解“角色互斥”和“角色继承”？

A. 得分点

（1）静态角色互斥是用户的不同角色之间不冲突；动态角色互斥是在会话选择时，角色与主体任意一个角色都不冲突。5 分

（2）角色继承表明了角色的组织关系，体现了访问权限的继承。 5 分

B. 参考答案

静态角色互斥：只有当一个角色与用户所属的其他角色彼此不冲突时，这个角色才能授权给该用户。它发生在角色分配阶段。动态角色互斥：只有当一个角色与一个主体的任何一个当前活跃角色都不互斥时，这个角色才能成为该主体的另一个活跃角色。它发生在会话选择阶段。

角色继承。在 RBAC 中，定义了这样一些角色，它们有自己的属性，但可能还继承了其他角色的权限。角色继承是将角色组织起来，自然反映系统内部角色之间的权利、责任关系。角色继承可以用“父子”关系来表示，可见教材图 5.6。角色 2 是角色 1 的“父亲”，它包含角色 1 的权限，处于最左侧的角色拥有最大的访问权限，越靠右侧的角色拥有的权限越小。