**第七章习题答案**

**1.什么是数据库安全？它包含哪些内容？**

**参考答案：**

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。

数据库系统的安全性问题包括用户身份认证，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以及分布式数据库安全等。

**2.什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。

**3.列出数据库系统中常用的安全机制，并对其作用进行简要说明。**

**要点：（1）身份认证，作用是防止非法用户的访问；（2）访问控制，限制用户或进程的访问能力或范围；（3）加密，保证数据库文件的机密性；（4）审计，监视记录数据库系统中的操作，用于非法访问的追查与漏洞扫描；（5）推理控制与隐通道分析，分析信息流动方向与非法信息流，从而发现安全问题；（6）安全恢复，将系统中数据从错误状态恢复到正确状态。**

**参考答案：**

（1）身份认证机制。身份认证是系统防止非法用户进入的第一道防线，即识别系统合法授权用户，防止非授权用户访问数据库系统。在开放的多用户系统环境下，对于要求访问数据库系统的用户，系统首先要求用户提供身份标识或鉴别信息进行身份认证，只有通过认证的用户才能进入系统。

（2）访问控制。访问控制是数据库安全最基本、最核心的技术。它是通过某种途径显式地准许或限制用户或进程的访问能力或范围，以防止非法用户的侵入或合法用户的不慎操作所造成的破坏。

（3）加密机制。一方面，由于数据库在操作系统下都是以文件形式进行管理的，入侵者可以直接利用操作系统的漏洞窃取数据库文件或篡改数据库文件的内容；另一方面，数据库管理员可以任意访问所有数据，往往超出了其职责范围，造成安全隐患。因此，数据库的保密问题不仅包括存储的敏感数据保密问题，还包括数据传输过程中的保密和控制非法访问问题，保密数据即使不幸泄漏或丢失，也不会造成泄密。同时，由于用户可以用自己的密钥加密自己的敏感信息，那么对于不需要了解数据内容的数据库管理员而言，他也是无法进行正常解密的，从而实现了个性化的用户隐私保护。

（4）审计机制。数据库审计是监视和记录用户对数据库所施加的各种操作的机制。通过审计可以把用户对数据库的所有操作自动记录下来放入审计日志中，这样数据库系统可以利用审计跟踪的信息，再现导致数据库现有状况的所有事件，找出非法存取数据的人、时间和内容等，以便追查有关责任。同时，审计也有助于发现系统安全方面的弱点和漏洞。审计日志对于事后的检查是非常有效的，但粒度过细的审计是非常浪费时间和空间的，因此数据库系统往往将其作为可选特征，允许数据库系统根据应用对安全性的要求，灵活地打开或关闭审计功能。

（5）推理控制与隐通道分析。在数据库系统中，恶意用户可以利用数据之间的相互联系推理出其不能直接访问的数据，或从合法获得的低安全等级信息或数据推导出高安全等级内容，从而造成敏感数据泄漏的一种安全问题，这种推理过程称为推理通道。推理控制就是检测和消除推理通道。推理控制方法分为四种：语义数据模型方法，形式化方法，多实例方法和查询限制方法。在数据库系统中的隐通道是指一个用户通过违反系统安全策略的方式传输信息给另一个用户的方法。它通过系统原本不用于数据传输的系统资源来传输信息，并且这种通信方式往往不被系统的访问控制机制所检测和控制。隐通道分析就是找出系统中可能存在的隐通道，其本质就是对系统中的非法信息流进行分析。原则上，隐通道可以在系统的任何一个层次进行，但分析的抽象层次越高，越容易在早期发现系统可能引入的安全问题。

（6）安全恢复机制。尽管数据库系统能够采取多种安全措施保证并发事件的正确执行，阻止数据库的安全性和完整性被破坏，但信息系统难免由于硬件故障、软件错误、操作人员失误或恶意攻击，造成数据库系统被破坏，这些必将导致数据库中的部分或全部数据的损坏或丢失。因此，数据库系统必须有一种将数据库从错误状态恢复到某一已知的正确状态的机制，把损失降到最低，这个机制就是数据库系统的安全恢复机制。

**4.数据库加密可以通过什么方式实现？可以实现哪些层次的数据加密粒度？**

**要点：（1）库内加密和库外加密；（2）文件、记录、表、字段或数据项。**

**参考答案：**

按照加密部件与 DBMS 的不同关系，数据库加密方式可以分为库内加密和库外加密。库内加密是在 DBMS 内核层实现加密，加解密过程对用户与应用透明，即数据进入DBMS 之前是明文，DBMS在数据物理存取之前完成加解密过程。库外加密是在DBMS 之外实现加解密，DBMS 管理的是密文，加解密过程可以在客户端实现，或由专门的加密服务器完成。

数据库系统的数据加密情况比较复杂，根据应用场合的不同，可分别选取以文件、记

录、表、字段或数据项作为加密的基本单位。

**5.分析安全审计在数据库系统中的作用。**

**要点：（1）审计数据产生和用户相关标识；（2）对正在发生的安全违规事件做出实时响应；（3）分析潜在或实时发生的安全违规事件；（4）对于施行安全审计的范围进行配置；（5）安全审计中相关记录的存储。**

**参考答案：**

安全审计数据产生。安全审计数据产生是指记录安全功能控制下发生的相关安全事件。它包括审计数据产生和用户相关标识。

安全审计自动响应。安全审计自动响应是指当安全审计系统检测出一个安全违规事件（或是潜在的违规）时，采取自动响应的措施。响应包括报警或行动，例如实时报警的生成，违规进程的终止，中断服务，用户账号的失效等，或及时通知管理员系统发生的安全事件。

安全审计分析。安全审计分析是指对系统行为和审计数据进行自动分析，发现潜在的或实际发生的安全违规事件。安全审计分析直接关系到能否识别真正的安全违规事件，它包括四个组件：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。

安全审计浏览。安全审计浏览是指经过授权的管理人员对审计记录的访问和浏览。数据库安全审计系统需要提供审计浏览的工具，通常审计系统对审计数据的浏览由授权控制，审计记录只能被授权的用户有选择地浏览，包括一般审计浏览、受限审计浏览和可选审计浏览，能够按照逻辑关系查询和排序。

安全审计事件选择。安全审计事件选择是指管理员可以从可审计的事件集合中选择接受审计的事件或不接受审计的事件，一个系统通常不可能记录和分析所有的事件，因为选择过多的事件将无法实时处理和存储，所以安全审计事件选择的功能可以减少系统开销，提高审计的效率。此外，因为应用场合的不同，所以需要为特定场合配置特定的审计事件选择。安全审计系统能够维护、检查、修改审计事件的集合，并能够通过选择性审计组件筛选对哪些安全属性进行审计。

安全审计事件存储。安全审计事件存储是指对安全审计跟踪记录的建立、维护，并保证其有效性，主要包括：受保护的审计跟踪存储、审计数据有效性的保证和预防审计数据丢失。审计系统需要对审计记录、审计数据进行严格的保护，防止未授权的修改，还需要考虑在极端情况下保护审计数据的有效性。审计系统在审计事件存储方面遇到的问题通常是磁盘用尽，单纯采用覆盖老记录的方式是不够的。审计系统应能在审计存储发生故障时或在审计存储即将用尽时采取相应的动作。

**6.如何实现数据库备份？需要注意哪些问题？**

**要点：（1）日志，应当注意日志需要在操作进行之前写入，说明原因；（2）数据备份。选取备份方式时要注意系统高可用与备份副本一致性之间的权衡。**

**参考答案：**

（1）日志。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。日志文件的内容包括：事务的开始标记，事务的结束标记，事务的所有更新操作。对于数据库操作日志，包括的信息有：事务的标识（标明是哪个事务），操作的对象，操作前数据的旧值（对插入操作而言，此项为空值），操作后数据的新值（对删除操作而言，此项为空值）。引入日志后，对数据库的修改操作实际上包含两部分：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，即必须先将修改操作记录到日志中，然后执行修改操作。这是因为，如果先修改数据库后写日志，有可能在这两步操作之间发生故障，这样就无法恢复修改操作了。

（2）数据备份。日志可以提供针对事务故障和系统故障的数据恢复，但为了在发生介质故障造成磁盘上数据丢失时也能进行数据恢复，通常还需要采用数据备份技术。数据库管理员定期将整个数据库复制到一个磁盘或磁带上保存。根据备份时系统状态的不同，备份可以分为静态备份（冷备份）和动态备份（热备份）。静态备份是在系统中无运行事务时的备份。这种备份方式简单，并且能够得到一个一致性的副本，但会降低数据库的可用性。动态备份是指备份期间允许对数据库进行存取或修改，即备份和用户事务可以并发进行。动态备份可以克服静态备份的缺点，即它无须等待正在运行的事务结束，也不会影响新事务的运行。但是备份结束时后援副本上的数据不能保证正确有效。

**7.数据库故障有哪些？对事务或数据有什么影响？**

**要点：（1）事务故障。事务没有顺利完成，可能引发死锁或数据错误；（2）系统故障。丢失缓冲区的数据，破坏数据库的原子性与持久性；（3）介质故障。破坏事务的原子性和持久性。**

**参考答案：**

（1）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。夭折的事务可能已经对数据库执行了部分操作，从而破坏了事务的原子性。发生事务故障的原因包括：输入数据有误造成运算溢出（如以 0作为除数），或违反了某些完整性限制发生锁死等。

（2）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，操作系统故障，DBMS 代码错误，突然停电等。发生系统故障时，由于系统需要重新启动，数据库缓冲区的信息全部丢失，但存储在外部存储设备上的数据未受影响。发生系统故障后，一些夭折事务的部分执行结果可能已经写入磁盘上的数据库，也有可能对数据库的更新结果还在缓冲区中，未能及时写入磁盘数据库，因此系统故障破坏了数据库的原子性和持久性。

（3）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。这类故障对数据库的破坏最大，它会破坏磁盘上的物理数据库，导致对数据库的更新结果丢失，并影响正在存储数据的所有事务，因此，介质故障破坏事务的原子性和持久性。

**8.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。**

**参考答案：**

事务故障的恢复**。**事务故障导致事务非正常终止，夭折事务的部分执行结果可能已更新到物理数据库中，破坏了事务的原子性。恢复子系统在不影响其他事务运行的情况下，强行回滚该事务，具体的做法为：利用日志文件撤销（UNDO）此事务已对数据库进行的修改，使得该事务好像根本没有启动一样。通常的做法是逆向扫描日志文件，对于日志记录的事务修改操作，将修改前的值写入数据库。

系统故障的恢复。发生数据库故障后，数据库缓冲区的内容都将丢失，所有运行的事务都将非正常终止，这将导致一些尚未完成的事务的部分修改执行结果已经写入了磁盘的数据库，而有些已完成事务对数据库的修改还留在缓冲区中，尚未写入磁盘的数据库中，从而造成数据库处于不正确状态。恢复子系统必须在系统重新启动后，让所有非正常终止的事务回滚，强行撤销（UNDO）所有未完成的事务，以保持事务的原子性，重做（REDO）所有已提交的事务以保持事务的持久性，从而保证数据库恢复到一致性的状态。重做的过程是正向扫描日志，对于事务的每一个修改记录，将修改后的值写入数据库。为了提高系统故障恢复的效率，可采用具有检查点（Checkpoint）的系统故障恢复技术。

介质故障的恢复。介质故障破坏物理数据库，使得所有已提交的事务的结果不能持久保存，并影响正在存储这些数据的事务，破坏事务的原子性和持久性，是最严重的一种故障。介质故障的恢复不仅要使用日志，还要借助于数据库备份。对于静态备份，恢复数据库备份后，数据库即处于一致性状态，然后利用日志重做故障前已经完成的事务，就能将数据库恢复到故障时刻相一致的状态。对于动态备份，恢复数据库备份后，数据库并不处于一致性状态，还需要根据日志文件，利用系统故障恢复的方法，撤销备份结束时尚未完成事务对数据库的修改操作，并重做故障前已完成的事务，将数据库恢复到与故障时刻相一致的状态。

**9.数据库安全和操作系统安全有什么关系？简要说明。**

**要点：（1）数据库系统可以继承一些操作系统文件管理的安全机制；（2）说明数据库安全与操作系统安全之间的差异；（3）数据库安全对数据管理的程度更细，控制的对象更多。**

**参考答案：**

数据库系统最初的数据管理是依靠操作系统的文件管理功能，利用访问控制矩阵，实现对各类文件的授权读写和执行等，同时还依靠操作系统的监控程序进行用户登录和口令鉴别的控制。数据库系统被广泛使用后，虽然原来用于操作系统文件管理的一些保护措施可以借用到数据库系统的安全保护中，但数据库安全和操作系统安全之间存在以下差异：

（1）数据库保护的对象类型更多，不仅仅是文件。

（2）数据库中数据的生命周期较长，其安全将涉及不同层次，如：文件、数据库记录和记录中的数据项等。

（3）数据库系统保护的对象可能具有复杂的结构，某些对象可能反映同一物理对象，而操作系统保护的是实际资源。

（4）不同的结构层，如数据库的内模式、概念模式和外模式，要求不同的安全防护。

（5）数据库安全涉及数据的定义和数据的物理表示。

从这些差别可以看出，数据库安全是基于操作系统安全之上的，但比操作系统安全的要求更高和更复杂，其对数据管理的程度更细，控制的对象更多。