9.8.6　审计追踪

审计追踪（audit trail）是对于应用程序数据的所有更改（插入、删除和更新）以及某些信息（诸如哪个用户执行了更改和什么时候执行的更改）的日志。如果应用程序的安全性被破坏了，或者即使安全性没有被破坏但是一些更新被错误地执行了，那么审计追踪能够帮助找出发生了什么，以及可能是由谁执行的操作，并且帮助修复由安全漏洞或错误更新所造成的损害。

例如，如果发现一名学生的成绩不正确，则可以检查审计日志，以找出该成绩是什么时候以及如何被更新的，并找出执行这个更新的是哪个用户。然后，大学还可以利用审计追踪来跟踪这个用户所执行的所有更新，从而找出其他的错误或欺骗性的更新并随后将它们更正。

审计追踪还可以用于探查安全漏洞，在安全漏洞中用户的账户易受到攻击并被入侵者访问。例如，在用户每次登录时，他可能被告知在审计追踪中从最近一次登录开始所做过的所有更新，如果用户发现一个更新并不是他所执行的，则有可能该账户已被攻击了。

可以通过在关系的更新操作上定义适当的触发器来创建一个数据库级的审计追踪（利用标识用户名和时间的系统定义变量）。然而，很多数据库系统提供了内置的机制来创建审计追踪，这样使用起来就更加方便了。创建审计追踪的具体细节随数据库系统的不同而不同，详细内容可参考数据库系统的用户手册。

数据库级的审计追踪对于应用来说通常是不够的，因为它们常常无法追踪到应用程序的终端用户是谁。另外，它是在一个较低级别以关系中元组更新的方式来记录更新的，而不是
445 在较高级别以业务逻辑的方式来记录更新的。因此，应用程序通常创建一个更高级别的审计追踪，例如，记录由谁在何时执行了什么操作，以及请求是从哪个 IP 地址发起的。

一个相关的问题是如何保护审计追踪本身，防止它被破坏应用程序安全性的用户所修改或删除。一种可能的解决方案是将审计追踪拷贝到另一台入侵者无法访问的机器中，审计追踪中的每条记录一旦生成就被立即复制。更健壮的解决方案是使用如第 26 章中所述的区块链技术；区块链技术将日志存储在多台机器中，并使用散列机制，使得入侵者很难在未被检测到的情况下修改或删除数据。

9.8.7　隐私

在这个可以在线获取越来越多的个人数据的世界里，人们也越来越担心他们的数据隐私。例如，大多数人都希望他们的个人医疗数据保持私密而不会被公开暴露。然而，这些医疗数据又必须开放给治疗病人的医生和急救医疗技术人员。许多国家都具有针对这种数据隐私的法律，定义了数据在什么时候以及对谁可以公开。违反隐私法在某些国家可以导致刑事处罚。必须谨慎创建访问这种隐私数据的应用程序，谨记隐私法。

另一方面，聚集的隐私数据在许多任务中都可以扮演重要的角色，比如检测药物的副作用，或者发现流行病的蔓延。如何使这些数据可以为执行这种任务的研究人员所用，而又不侵犯个人的隐私，这是一个重要的现实问题。作为一个示例，假定一家医院隐藏了患者的姓名，但是给研究人员提供了患者的出生日期和邮政编码（这二者可能对研究人员都有用）。在很多情况下，仅使用这两条信息就可以唯一标识出患者（使用来自外部数据库的信息），从而侵犯了他的隐私。在这种特定情况下，一种解决方案是只提供地址和出生年份而不提供出生日期，这对于研究人员可能就足够了。但这提供不了足够的信息来唯一标识