数据库安全

数据库安全

随着计算机技术的飞速发展，数据库的应用十分广泛，深入到各个领域，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。

数据库安全的迫切性

数据库平台缺少有力的本地加密、监测、评估和管理工具来满足这些新的安全要求。最近又出现了威胁数据库安全的侧面 SQL 注入技术。利用这种技术，黑客可以迫使数据库执行他的命令，而这样的攻击不需要本地访问数据库。此外，有调查显示数以千计的微软 SQL 服务器和甲骨文数据库服务器可以通过 Internet 进行访问，它们缺少关键的更新补丁，很容易受到攻击。

- 数据敏感性加强 数据库安全倍受重视
- 新 SQL 注入技术威胁 Oracle 数据库
- 调查显示 数据库服务器易遭攻击

数据库安全防范措施

要完全保证数据库的安全，就需要把这个任务分为以下四个方面以确保进行全面的检查:服务器安全、应用程序安全、数据库连接、数据库和表格访问控制。数据库压缩防护产品可以阻止已知攻击，预防未授权的用户访问并检测异常用户行为。它是入侵防御系统（IPS）和网络行为异常检测（NBAD）系统的一种交叉产品。另外，在保持数据库安全得到控制的同时，也需要在这个过程中考虑成本节约。

- 保证数据库安全的几个简单步骤
- 数据库压缩产品可以有效防护数据丢失吗？

- 数据库安全投资平衡

数据库加密

除了管理可能存在的兼容性、可靠性和运行需求问题外，安全部门还要面对大量的加密选项、密钥管理缺陷、以及应用程序的综合需求。数据库加密决不容轻视，具备一些知识和规划就会对确保一个项目的成功大有帮助。任何加密工作的第一步都是确定保护什么数据，以及要防范的对象是谁。

- 数据库加密的细节
- 保密数据应该编入索引或作为索引关键字吗？

数据敏感性加强 数据库安全倍受重视

不久前，“数据库安全”几乎是一种矛盾，但今天，对审计和对客户信息违规进行打击的要求迫使公司不得不高度重视谁访问了敏感数据和他们做了些什么。

那对于安全管理人员来说是个好消息，他们现在越来越受重视，对于数据库安全厂商来说也是个好消息，他们看到了人们对这个现在还很小(一般估计第三方产品少于 1 亿美元)，但正在发展中的市场的越来越多的兴趣。

“这个领域的许多公司在两年里每年翻了一倍，”一个位于 Boston 的 Yankee Group 高级分析师 Andrew Jaquith 说。“在 2007 年他们很可能再翻一倍。在资金优势方面它是个大领域。”

这个市场包括三种产品：

数据库检测/审计：公司用这些工具来观察未经许可或不寻常的访问活动，并不用消耗数百或上千的人时去细查 log 文件就可以产生全面的审查报告。这些供应商包括 Application Security, Inc.，Embarcadero，Guardium，Imperva，IPLocks. Lumigent technologies，RippleTech，Sentrigo，Symantec 和 Tizor Systems。“数据库本身并不能智能到能查看通过网络的可疑活动或是否授权用户执行一个命令一百万次，”位于 Cambridge 的 Forrester 研究机构的一个首席分析师 Noel Yuhanna 说道。“这就是为什么你需要有这些工具。”

脆弱性评估：来自于 Application Security 和 Next Generation Software 这样的公司的专门的 VA 扫描器，评估数据库的安全强度，检测安全漏洞和错误配置。

加密：采用集中的管理、策略创建和强大的密钥管理的高度粒状加密。厂商包括 Protegrity，Ingrian Networks 和 Application Security。

增强的安全敏感度拉动了市场的发展，因为违规一个接着一个的揭露出来破坏了客户的信任，还有对有点模糊的调整遵从性检查压力的要求也带动了市场发展。

“单独的最大的驱动是 SOX;它改变了公司的审计要求，并且我们看到了一点点的 PCI，”位于 Stamford 的 Gartner 公司的研究副总裁 Rich Mogull 说。“尽管规范没有明确的说出我们正在谈论的是什么，但是他们最终推动你朝这方向前进。”

“这个基础驱动本身并不做审计，”Jaquith 说道。“它有些尴尬，并且有名誉风险。”

数据库平台缺少有力的本地加密、监测、评估和管理工具来满足这些新的安全要求。此外，大型的不同种类的组织经常有多种多样的数据库平台。Oracle 和 Microsoft SQL Server 越来越好，但还有很长的路要走。

“明年有很大空间能看到数据库厂商的更多的活动，或者通过合作，或者只靠他们自己，”位于 Framingham 的 IDC 公司的研究主任 Charles Kolodgy 说道。

Yuhanna 看到了明确的迹象显示监测和审计市场正在步入下一阶段，既然公司认识到了他们的价值。他期望看到大型公司投资 50 至 100 个设备部署。

另一方面，数据库加密技术在解决方案的列表上仍然是相对较低的，尽管对数据被盗和为加密数据解密的关注在大多数情况下违背了批露法。尽管改进了工具，部署和管理却仍然很困难。分析家警告说数据库加密是一个两三年的事情。遗留系统尤为严重。

“数据库加密技术是人们购物列表上的第三项，”但是市场将继续发展，Kolodgy 说道。“没有人靠异想天开来加密。要很清楚的了解需求;要有很清楚的描述。”

“我会说只有 5%在做数据库级别的加密，”Yuhanna 说道。“它太困难了。”

执行加密的很重要的一部分是选择，要了解需要保护什么。你可以加密用户的信用卡和社会安全号码，但要以纯文本的形式显示姓名和地址。

分析家们在建议方面意见有些不同，但是一般推荐积极监测，这会得到最大的投资回报率。再有推荐选择域级别的加密。

“确定你有什么类型的敏感数据，什么类型的数据库和有多少，”Jaquith 说道。“简单的四处看看和查询数据库是有用的，但是你需要实证。利用扫描工具来探测你的数据，指出什么是敏感的。”

“敏感的用户信息就像是石棉一样，”他说。“我们很多年都在盖储存它的房子，但直到最近空运的时候才发现它的毒性。”

（作者：Neil Roiter　来源：TT 中国）

新 SQL 注入技术威胁 Oracle 数据库

数据库安全专家 David Litchfield 正在研究利用多种不需要输入的 PL/SQL 程序的新方法。他把这型技术描述为侧面 SQl 注入，可以对 Oracle 数据可进行远程攻击。

这种攻击利用一些普通的数据类型，包括 DATE 和 NUMBER，它们不需要使用用户的输入，所以通常不被认为可以攻击。但是，Litchfield 在他关于侧面注入攻击的新文章中写道，使用一点创造性译码和一些 Oracle 数据可管理系统工作方式的知识，黑客就可以操作一些一般的功能。

Litchfield 是英国 NGS Software 公司的创始人之一，他说这个问题可能不会那么容易的攻击，但是特殊情况下，它可以被用于向数据库传输任意 SQL 命令。

PL/SQL 是 Oracle 公司的 SQL（structured query language）的延伸。

“总之，如果使用 SYSDATE，那些不需要用户输入的功能和程序就有可能受到攻击。这里的教训总是会得到验证，防止这类攻击进入你的代码。第二个教训是 DATE 或者 NUMBER 不应该再被认为是安全的，也不会和注入携带者一样有用：这篇文章证明，他们是。”他写道。

这类攻击工作模式如下：使用 SYSDATE 功能，黑客可以使用 ALTER SESSION 权限欺骗 SQl 编译器，接受任意的 SQL 数据作为 DATE 数据类型的输入。DATE_PROC 使用变量 V_DATE 在调用 SYSDATE 功能后，设置数据。尽管如此，通过改变讨论（altering the session）和插入 SQL 命令，黑客可以迫使数据库执行他的命令。

黑客的攻击不需要本地访问数据库。

“可以通过远程完成，例如，借助一个 Web 应用程序，通过 SQL 注入漏洞，但是不是直接进入。” Litchfield 在邮件采访中，如此说。“首先，我们攻击注入点来执行促进功能，这允许我们运行任意 SQL，然后在这里可以使用这项技术。”

Litchfield 的文章中有意思的一点是 DATE 和 NUMBER 等数据类型被认为是“安全”的事实，意味着他们还没有受到攻击。最近几个月中，这类攻击越来越多，研究人员已经开始深入研究流形的应用程序，在有些情况下发现了严重的新型攻击携带者。

去年夏天，Watchfire 公司的研究人员，现在是 IBM 的一部分，他们发现攻击摇摆指示器的方法，这是一个被认为不能攻击的平常的程序失误。IBM 的 ISS 部门的研究人员 Mark Dowd 发表了一篇论文，详细指出了攻击 NULL 指示器解除参照。

对他来说，Litchfield 的新方法不是通过长时间的脑子里的工作，而是通过看电视产生的。

“同时，观看‘Bones’的一段情节，里面发生的一些事情让我想到不要接受默写认为真实东西，比如，在这种情况下，通过 DATE 和 NUMBER 数据类型进行 SQL 注入是不可能的。所以坐下来，想一想我在文章中提出的一些技术。”他说。

（作者：Dennis Fisher　译者：Tina 来源：TT 中国）

调查显示 数据库服务器易遭攻击

安全研究领域的权威研究人员 David Litchfield 曾在 07 年十一月份发布一份报告，显示数以千计的微软 SQL 服务器和甲骨文数据库服务器可以通过 Internet 进行访问，它们缺少关键的更新补丁，很容易受到攻击。

Litchfield 是位于英国的 Next Genreration Security 软件公司的常务董事。他统计了互联网上没有防火墙保护的微软 SQL Server 和 Oracle 数据库服务器的数量。这份名为“数据库暴露调查 2007”的报告中指出，约 36.8 万台微软 SQL Server 和 12.4 万台 Oracle 数据库服务器可以通过 Internet 直接访问，而且没有防火墙保护。该调查上一次进行的时间是 2005 年。

“作者看来，这些结果表明了一个重大的风险”，Litchfield 说，“虽然不好说这些系统中有多少是用于商业功能的，但近 50 万台可访问的服务器无疑让黑客们和罪犯们有机会来获得这些系统的访问权限和敏感信息。”

Litchfield 说，66%的甲骨文数据库服务器运行的版本，是公认容易受到严重攻击的旧版本系统软件。他说，82%的 SQL 服务器运行的是 SQL Server 2000 版本，并且仅有 46%的运行了补丁程序 SP 4,剩下的仅运行了补丁程序 SP 3a 甚至更低版本。他还说，数据库管理员们并没有安装一些热修复补丁程序（介于两个正式发布的补丁程序之间的小补丁），而是等着正式发布的补丁程序。

“很多数据库管理员可能根本不知道他们的系统可以通过互联网直接进行访问。”Litchfield 说。

另外，自从 2005 年进行过调查后，存在风险的 SQL Server 数据库的数量明显增加了，Litchfield 说。在 2005 年，没受保护的 SQL 服务器约有 21 万，而目前的调查显示有 36.8 万台存在风险。

参加了 2007 年甲骨文开放世界会议（OpenWorld 2007）的数据库管理员们不会惊讶于这项调查结果。很多时候，数据库管理员安装了一个测试服务器，却根本没有意识到服务器可以通过 Internet 被访问，很容易受到攻击，Tim Spoddard 说。Tim 是一家中西部零售商的 DBA。Spoddard 建议，“这是一个很好的提醒：好好检查一下你的系统。在当今这时代，最好隔离攻击区域，防止数据泄露。”

Andy Lehman 是加州圣何塞的一名 DBA。他说大部分可以通过互联网访问的数据库服务器可能不包含敏感信息。尽管如此，它们仍应该被锁定，而且还应该与关键系统分离。

“如果它们不更新并且存在关键的缺陷，那么尽管他们本身并没有什么值得盗取的信息，但它们仍可以作为攻击者的跳板。”他说。

Litchfield 说，数据库服务器应该经过测试来保证它们不能通过互联网来访问。同时，应该由防火墙来控制所有从外部对数据库服务器的访问，防火墙应仅允许设置好的一部分 IP 地址或地址段访问。

（作者：Robert Westervelt 译者：Shirley 来源：TT 中国）

保证数据库安全的几个简单步骤

数据库及其包含的信息仍是黑客试图攻击的目标。黑客希望利用在数据库驱动的应用程序中的许多广泛传播的安全漏洞。这些漏洞许多是由不良设置或者实施造成的。下面是最常见的五个与数据库相关的安全漏洞:

•弱的密码策略

•SQL 注入

•交叉站点脚本

•数据泄漏

•不适当的错误处理

令人难以置信的是，企业仍经常使用默认的或者软弱的口令来保护像数据库一样重要的在线资产。但是，这是一个很容易解决的问题。补救措施是强制执行强大的口令政策。也就是说，口令要定期变换，口令长度最少为 10 位数并且包含字母和符号。采用这种政策，你将关闭攻击者同向你的数据的方便之门。

SQL 注入也依靠软弱的数据库实施，特别是在如何向数据库发送 SQL 请求方面的实施。如果这个数据库接受了用户提供的不干净的或者没有经过验证的数据产生的 SQL 请求，这就会为 SQL 注入攻击敞开大门。例如，通过修改从基于网络的格式受到的信息，攻击者能够提供恶意的 SQL 请求并且把指令直接发送到数据库。

要防止这种类型的攻击，在让这些数据接近你的脚本、数据访问程序和 SQL 查询之前，保证所有用户提供的数据是合法的是非常重要的。验证和清洁从用户那里收到的数据的另一个理由是防止交叉站点脚本攻击。这种攻击能够用来攻破连接到一个 Web 服务器的

数据库。黑客通过一个网络蠕虫把 JavaScript 等客户方面的脚本注入到一个网络应用程序的输出中。这些脚本用于收集 cookie 数据。这些数据经常被错误地用来存储用户账户登录信息等资料。

一个经常被忽略的问题是什么时候建立一个数据库应用程序是泄漏数据。这是敏感数据被非故意发送的地方或者使之可用的地方。这个错误将导致不能保证访问数据库备份磁带的安全和控制这种访问。通常，更敏感的数据产生于有关数据的合法查询的答案，就像从医疗处方判断疾病一样。常用的解决方案是监视查询方式以检测这种行动。

与数据泄漏密切相关的是在数据库出现错误时不适当地处理这些错误。许多应用程序显示了详细的信息。这些错误信息能够泄漏有关数据库结构的信息。这些信息能够用来实施攻击。要尽一切手段把这个错误登记在你自己的记录中，保证你的应用程序不向用户或者攻击者返回任何有关这个错误的详细信息。

要完全保证你的数据库的安全，你要把这个任务分为以下四个方面以确保进行全面的检查:

•服务器安全

•应用程序安全

•数据库连接

•数据库和表格访问控制

数据库服务器需要与其它任何服务器一样加强以保证任何恶意黑客都不能通过操作系统的安全漏洞攻击数据库。更适宜的方法是数据库应该位于其自己的应用层防火墙之后。

要帮助保证数据库连接的安全的过程和定义访问控制，你应该创建一个数据流动图表，跟踪数据如何流过应用程序的过程。接下来，找到数据进入或者退出另一个应用程序的地方，并且检查为这些进入点和退出点分配的信赖等级。还要定义需要访问这个系统的

外部用户或者处理要求的最低权限。把安全作为关键的推动因素来设置和建立你的数据库将保证你的数据库处于安全状态。

（作者：Michael Cobb　来源：TT 中国）

数据库压缩产品可以有效防护数据丢失吗？

问：我听说了数据库压缩防护系统。他们是什么呢？这个的市场的成熟度怎么样？

答：压缩防护的目的是预防未授权的数据访问和使用。企业存储的个人数据日益车成为黑客和有组织犯罪的第一位的攻击目标。数据保护正需要立法调整和遵守，而这就是原因之一。虽然数据库会产生并维护处理日志，这些日志的目的是防止或识别恶意行为，因此需要控制数据访问和使用的多种方法。

数据库压缩防护产品是入侵防御系统（IPS）和网络行为异常检测（NBAD）系统的一种交叉。当提到数据库防火墙的时候，你可能会听到这些名称，但是这并没有涵盖它所有的功能。它可以阻止已知攻击，预防未授权的用户访问并检测异常用户行为。为了控制数据运转，很多产品都需要一个转折期，这样就需要设定基线来描述和规范用户行为。这样的设置可以根据变换的商务和用户需求而调节。例如，如果用户或 Web 应用开始请求异常数据，数据库压缩检测产品可以阻止这样的请求，或者警告管理员，而管理员可以决定它是否适合规则设置，或者需要对事件进行深入调查。

数据库压缩防护产品可以通过以下两种方法配置：在线或者带外。在线产品直接放在数据库服务器和连接孔之间，而带外的产品需要在交换机上使用连接孔分析器(SPAN)端口。SPAN 端口分析来自或去往数据库服务器。数据库压缩防护产品可以通过在黑客和数据库服务器之间断开网络链接，或者通过在恶意流量来能够到达数据库服务器放弃它来阻止攻击。

很明显，会出现假阳性问题，合法的流量可能会偶尔被阻止。这个问题的减轻需要数据库压缩防护产品具有灵活性，并且提供详细的报告。还有，系统管理员需要评估为防止可能的数据泄露影响和成本，而阻止合法商务进程带来的风险。

在这个领域，有几家知名的厂商，例如 Application Security Inc.， Imperva Inc. 和赛门铁克。虽然这是相对比较新的技术，当然价格不便宜。数据库压缩防护当然可以帮助完成法规遵从的，例如文档访问、职责分离以及用户行为审计。另一个你可能想要采用类似的技术是压缩检测，这种技术利用的是系统本身状态的可见性。这些产品可以实时分析网络流量的内容和有效载荷，他们可以在所有的通道上进行分析，例如 HTTP，FTP，即时通信 Internet 多线交谈和 P2P 通道。

（作者： Michael Cobb 译者：Tina TT 中国）

数据库安全投资平衡

数据库平台的大小和复杂程度不断地增长，特别是当涉及到安全的时候。很多平台都以及与任务的加密和密钥管理，第三方的产品整合的用户管理员附件和更多的 APIs 为特征。这些功能存在新产品漏洞和正在形成的自动化威胁，这就为目前和将来的数据库安全提出了挑战。

微软的 SQL 服务器、Oracle 数据库、IBM 的 DB2 和 MySQL 都有责任。更明确地说，他们每一个都为他们的数据库套件创建了一套功能，可以允许系统管理员创建并管理用户和群帐户，备份数据并在合适的时候打补丁。非常不幸的是，这些功能应产品而异。

这里是一些技巧，不但可以帮助保持数据库安全得到控制，也可以在这个过程中节约一些成本。

成本节约技巧 1：挑选一个平台并使它标准化。

工具的数量和管理员功能要求维护并管理企业数据库的持续增长。数据库公司已经开始建立附加的服务和产品附件，目的是扩展到中级市场。这种商业驱动产生了一些技术分支。例如，附加服务和组件增加了管理员劳动力的成本；多平台的结合只是使这个问题更加的复杂。标准化一个平台可以降低劳动力成本，减少可能的培训，可以把您放在一个有利的位置，在场上提供的价格中有更多的选择。从我的经验来说，如果你告诉他们出于竞争之中，这些人可能至少降价 10%。

微软和 Oracle 在他们的平台的升级加密和虚拟分割功能存在争议。Oracle 的虚拟私有数据库和微软的自定义数据规则允许你在 table 中指定用户在列级别的访问。加密评估建议经常是“深度防护。”如果加密数据到了错误的人手里，那么它仍然是安全的。这些厂商已经在排除外部较小的加密产品方面迈出了第一大步。

成本节约技巧 2：安装内置加密和数据访问功能。

这些大人物本来就比较无情，他们不喜欢在他们的市场上失去最小生境。假设大家都快速安装新的功能，那么在产品已有或将在一年内添加的功能上投资，就没有意义了。单凭经验的方法是当你买了数据库的更新后，确保它至少比平台整合提前至少两年。

说完这个，就期待“附加”厂商把他们的经精力集中在多平台密钥管理上面。除非 Oracle 和微软颠倒他们的商业模式，对于小厂商来说，这将一直是一个小的销售优势。

尽管对于不同的人来说，数据库安全的意思也不一样，但是所有人都同意企业的主要应用程序都需要不同级别的安全措施。日志管理和入侵检测/访问控制都包括在了应该遵守的原则中：支付卡行业数据安全标准（Payment Card Industry Data Security Standard，PCI DSS）奥克斯利和加利福尼亚商业公共安全标准，A.B. 1950。这些都要切数据库包含各种敏感信息备份，并以适当的格式保存日志。另外，规则要求企业监控数据访问和/或入侵。

成本节约技巧 3：关系亲密的物理/虚拟数据库

把企业数据库以亲密的关系存储，可以大大减少网络管理和潜在的网络为基础的安全组件。除了劳动力减少外，单单这一点就可以节约好几万美元的资本支出。单独来说，稳定的网络，然后安装一个系统，来管理单独的网段。

确保你的数据库已经有了目前的厂商的补丁，只是完成了战争的一半。大部分的应用程序和数据库入侵都利用了错误的配置和应用层逻辑。幸运的是，国家安全代理和互联网安全中心都公布了资料，帮助你向正确的方向前进。下一步是未定实际的数据库配置。设立合适的群访问控制、文件限制和加密的使用都不是简单的事情。甚至专家都比较难平衡安全和性能。太多的群限制可以导致发展负担的增加，同时，加密可能给 CPU 带来额外的 30%的任务。

成本节约技巧 4：使用结构测试咨询和漏洞工具

创建一个“今本位”数据库平台结构，应该与大部分的软件的发布时间相符，至少应该是两年一次。因为创建这样基线的频率很低，最好投资于一次性咨询－－他们可以给你可以使用的建议，而不是去买一些附加软件，在束之高阁。

漏洞测试时强制性。频率、深度和类型都可以改变。取决于数据库的使用和相应的应用程序，可能必须在三个层面扫描：网络或基础结构，平台和应用软件。每周一次的网络和平台扫描以及当应用程序改变时的应用层扫描，被认为是行业的最佳实践。所有数据库的漏洞测试应该多次、重复进行，而结构测试只在主要更新是进行就可以了。

成本节约技巧 5：研究产品指示图

最后但当然并非最不重要的一点是，理解数据库的志向非常重要。深入理解你的厂商的五年计划都很大的杀伤力，然而你应该熟悉未来两年版本中增加的内容。这就是，研究是非常关键的。Web 可能只发布下一个到来的内容，而不是将来发布中的改变。给你的你的零售商打电话，或者给厂商发送电子邮件，是向正确的迈出的一大步。这些步伐可以确保你减少过度的购买、减少内部用户发展和“权宜”工作区。

成本是每个数据库解决方案中应该考虑的因素，因为每一种选择附带而来的都是相应的劳动力和技术构成。识别和权衡与预算的 ROI 前景相结合的风险的威胁模式可以快速地发现你可以担负的防御。

（作者：　译者：　来源：TT 中国）（宋体 10，居右对齐）

数据库加密的细节

在信息安全工作中，企业数据库加密是最令人畏惧的工作了。除了管理可能存在的兼容性、可靠性和运行需求问题外，安全部门还要面对大量的加密选项、密钥管理缺陷、以及应用程序的综合需求。数据库加密决不容轻视，具备一些知识和规划就会对确保一个项目的成功大有帮助。

任何加密工作的第一步都是确定保护什么数据，以及要防范的对象是谁。我曾经合作过很多客户，他们都试图跳过这一步而直接进入技术配置。这些客户的数目之多，一定会让你大吃一惊。在实施技术之前，必须提前解决如下问题：

- 你想阻止数据库用户使用数据吗？
- 你想要保护数据不受外部攻击吗？
- 你需要保护所有的数据，还是仅仅是像信用卡数字那样的一列数据？

只有两种方法真正实用于加密技术，每一种都将直接决定着组织系统结构的选择。

媒体保护加密

第一种方法是媒体保护加密。在这种方式中，全部数据库都有可能被加密，其目的是保护数据库文件或内容，以防物理或虚拟方式窃取。这里需要注意的是有人会偷取数据库文件或者储存数据的媒体。如果你担心有人侵入服务器并窃取数据库文件，或是当你换出硬盘时丢失数据库文件，选择这种方法是相当正确的。尽管这种方法可能能够保护数据，防止系统管理员或其他有权访问保存数据库的地址的用户盗窃。但是，这种方法不能阻止数据管理员或者用户（或者任何侵入其账户的人）访问这些数据。

媒体加密是相当直接的，并有大量好产品和技术可供选择。由于是在数据库以外加密，因而它影响数据库性能的可能性就更小，也不需要对数据库或应用程序作出任何改变。一些数据库管理系统包括这样一种可供选择的加密技术：允许在数据表格或整个数据库水平上加密。或者，可以选择使用几乎任何一种高性能文件或文件夹加密工具。在这两种情况下，加密操作是在服务器上进行的，如果它超出可接受的限制以外，会反过来影响性能。这时就要考虑使用一种内嵌式加密设备，该设备带有专用硬件来加速加密进程。

加密和责任分离

第二种组织采用的方法的是责任分离加密。如果你的企业为了阻止管理员看到数据，以及其它类似情形的发生，需要对数据库中的信用卡数字进行加密，那么这是最好的选择。责任分离加密比对媒体保护加密要复杂得多；它包括保护数据，以防合法数据库用户盗窃，并要求数据库本身进行更多的改变。几乎每种情况下，这都意味着需要进行列级加密。如果列是一个单独的区域，不是一个主要的或是外部密钥，不依赖于其用于标定性能的系统结构，也不受限于范围搜索，那么对于加密而言，这就是一种不错的选择。反之，它仍然可以用于加密，但需要改变主要的数据库和应用程序。

既然你能够按照所构建的加密技术进行规划，那么为列级加密技术设计一个新的数据库的过程就是非常简单的。此外，一些含有繁琐的应用程序附件的遗留体系，需要一个主要密钥进行加密，对于这些体系，该项目将持续 2-3 年。大部分加密方案都中途破产，其难点是由密钥关系，指标和任何必要应用程序的改变决定的。

数据库加密的一些建议

虽然所有主要的数据库管理系统提供了列级加密，但是没有一个系统支持去除那些数据库默认的密钥。我的建议是尽量使用本地的加密性能，不要使用第三方密钥管理产品来将密钥从数据库中分离出来。该策略允许安全管理者，而不是数据库管理者，对密钥进行管理，支持责任分离。不论其他任何人告诉你什么，你都不要尝试加密主要密钥。最后，确定你真正得到了你期望的利益——数据库加密无法防止 SQL 入，并无法阻止一个有权进入的危险账户。

关于域加密，我的建议是：如果可能的话，尽量避免在现存的数据库中使用加密，而要在含有敏感信息的数据库中构建加密技术。比如，在将信用卡数据从现存系统中分离出来的时候，我的一些大型企业客户正采用信用卡数据来构建安全中心库，这些信用卡数据是用于交易的、并已经经过加密。如果需要在现存系统中分离职责，可以考虑使用媒体保护加密，然后可以添加另一种数据库安全技术——比如数据库活动监控——来实现责任分离。

(作者：Rich Mogull 译者：李娜娜 来源：TT中国)

保密数据应该编入索引或作为索引关键字吗？

问：我看到有的文章说，数据库的保密数据不应该把编入索引或作为索引关键字。这是什么意思？我应该采用什么最佳方案来保证在我的公司里不会出现这种问题？

答：数据库索引就像是课本的索引一样。他们提供对查找所要求数据的快速参考点。从而减少了数据库伺候器的负担并加快了数据检索的次数。在一个关系型数据库中，每一个表格都应该有一个作为索引的主键值，这个主键的唯一作用是在数据库的各记录间创建一个定义好的链接和一个独一无二的值。为了保证数据库的技术实现与商务规则相分离，这个主键值不应该有任何实际的意义。比如：一个银行客户的表格可能用一列来存储每一个客户独一无二的银行账户号码，这个号码可能作为主键的候选之一。每一客户数据的主键值都是不同的。

为了加快客户数据的检索速度，比如说，每个客户的银行帐户号码或社会安全号码可以被编入索引。这个设定允许银行职员使用这条特殊的信息来快速搜索数据库。然而,Core Security Technologies 公司的研究人员发现，这些索引是一种新技术攻击的对象。为了在数据库的索引运算方法中找弱点，攻击采用一系列嵌入的操作，然后从索引字段中提取数据。这些嵌入指令并不是攻击应用程序逻辑或代码的漏洞，所有数据库使用人员都可经常使用这样的嵌入指令。

最初的防范建议是不对保密数据使用索引。然而没有索引，数据检索是很复杂的。为了找到与银行帐号或社会安全号码相匹配的记录，数据库伺服器必须浏览所有表格，查找客户表格的每一行信息。而对于多表格相互间的复杂查询很大程度上取决于索引值。这些延迟会对大型商业数据库性能产生很大影响，可能会导致瘫痪。

不过，没有报导说这种攻击广泛存在，它只是一种似是而非的威胁。数据库管理员应该更加密切地监控日志文件来寻找异常反复的嵌入操作。应用程序防火墙也需要致力于探

测异常活动模式。对于新的数据库，设计者必须对数据模型和用户代码做出一些调整。对于必须进行索引的的每一列，都必须有一个对应的列来存储保密数据的散列值。然后，用这个散列值作为索引。这样，攻击者就不可能计算出保密数据的值了，从而有效地防止数据的攻击。通过搜索已编入索引的散列值，并将数据的散列值作为搜索准则进行传递，应用程序仍然能够有效地搜索保密数据。

（作者：Michael Cobb 译者：Shirley 来源：TT 中国）