symantec. press

网络安全专家

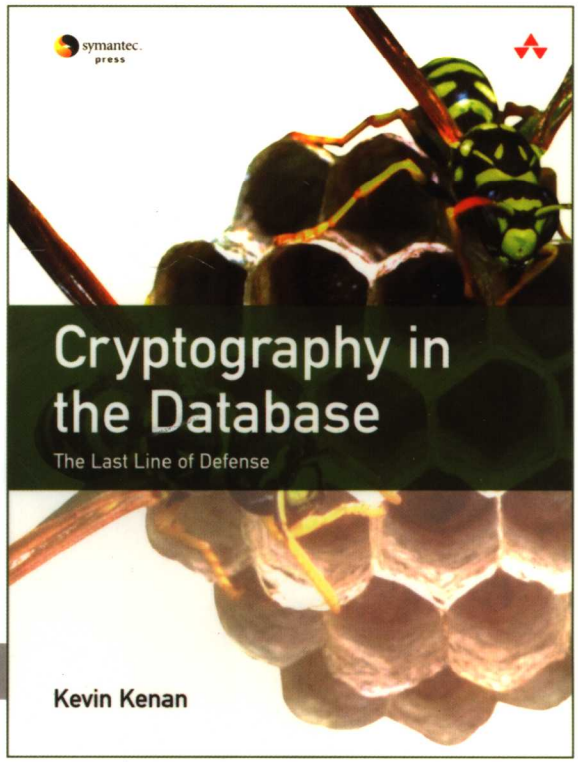
数据库加密
——最后的防线

数据库安全问题

数据库密码系统的设计

安全地实施密码系统所必需的开发过程

设计实现的示例代码



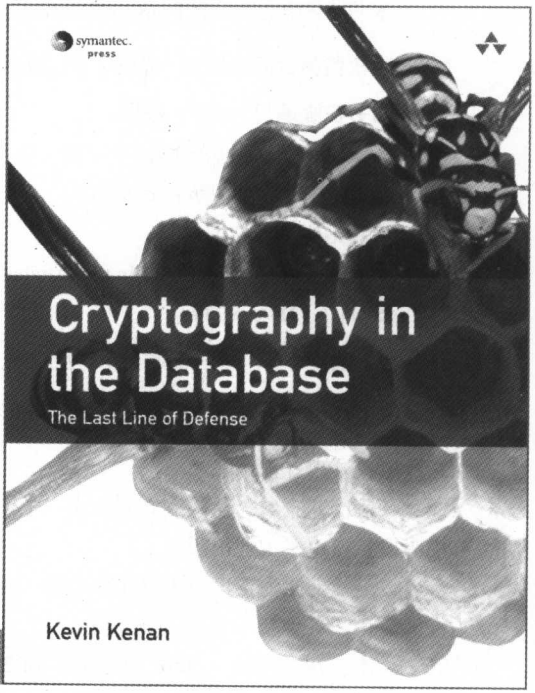
[美]Kevin Kenan 著
李彦智 马 超 林 滨 译
飞思科技产品研发中心 监制

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Symantec Expert

网络安全专家

数据库加密
——最后的防线



[美]Kevin Kenan 著
李彦智 马 超 林 滨 译
飞思科技产品研发中心 监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

EXPERT

内容简介

版权贸易合同登记号　图字：01-2005-6597

图书在版编目（CIP）数据

数据库加密：最后的防线 /（美）凯文（Kenan,K.）著；李彦智，马超，林滨译.
北京：电子工业出版社，2006.9
（网络安全专家）
书名原文：Cryptography in the Database：The Last Line of Defense
ISBN 7-121- 02993-6

Ⅰ. 数...　Ⅱ.①凯...②李...③马...④林...　Ⅲ.数据库－密码－加密　Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2006）第 089247 号

责任编辑：赵红梅
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京海淀区万寿路 173 信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：18.25　字数：408.8 千字
印　　次：2006 年 9 月第 1 次印刷
印　　数：6 000 册　　定价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：（010）68279077；邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn。
服务热线：（010）88258888。

致　谢

首先，我要感谢我的家人，感谢他们为此书的诞生所做出的巨大牺牲。在 Ella 出生的前几个月里，我正忙着编写本书的手稿；在很多个周末因为我要去工作，所以不能陪伴 Skyler；Stephanie 用她无私的爱容忍着我这个不称职的丈夫。我要对我的家人说："没有你们的无私支持，就没有这本书的问世。"

感谢 Symantec 出版社的 Linda McCarthy 和 Addison-Wesley 出版社的 Jessica Goldstein，是她们的热心促成了这本书的出版，还有 Frank Vella，她也为本书的出版提供了很多帮助。感谢 Christy Hackerd 接受了我的所谓"已完成"的手稿，并在天才的 Addison-Wesley 小组的帮助下，将手稿整理成书。

很多具有深刻见解的人都对这本书中的文字和代码进行过审阅和检查。特别感谢 Bob Bruen，AlanlCrassowski，Don MacVittie，Ulf T. Mattsson，Drew Simonis，Anton Stiglic 和 Mark R. Trinidad 等人，他们在几份手稿上所做的批注使这本书更加完善，我对此十分感激，并仔细考虑了如何更好地实现批注中所提到的内容。读者可以访问 http://www.kevinkenan.com 来获得与本书有关的最新消息和勘误信息。

还要感谢"Delta & Green Acres"星巴克咖啡店的员工们。在漫长的几个月里，每个周末的午后他们都热情地为我提供意大利特浓咖啡（Espresso）和电源，那种抿一口咖啡，再写几行代码的感觉真的很惬意。

最后，我还要深深地感谢俄勒冈州大学（University of Oregon）的 Emeritus Richard Koch 教授。他的耐心鼓励和讲解帮助我和一大批学生了解到了数学的魅力，我对密码学的追求之路就是从他的办公室开始的。

Kevin Kenan

读者意见调查表

您的意见是我们创造精品的动力源泉!

本次购书资料

书号：7-121- 02993-6　　书名：《数据库加密——最后的防线》

读者基本资料及意见

姓名_____ 性别____ 工作单位_____ 联系电话_____

联系地址_____ 电子邮件_____

一、下列对您使用计算机的描述，哪一种最接近您的状况？

□我是一个计算机的初学者，已开始学习使用计算机，但还不熟悉

□我能用独立的学习方式（如图书、网络）学习计算机的操作，并使用计算机

□我熟悉一般计算机的软硬件操作，但还想更深入

□我是个靠计算机技能上班的工作者，软硬件都是我的专长

□我不仅靠计算机吃饭，而且拥有顶尖的计算机技术

二、对于计算机技术类图书，您最在意下列哪些条件？（可复选二项）

□价格是否合理/便宜　□内容是否实用/充实　□印刷是否精美/彩色

□书中实例是否精彩　□知名的作者/出版社

三、您目前最常购买以下哪一类图书？（可复选）

□计算机基础入门　□操作系统/网络系统　□办公软件

□程序设计　□网页设计/网站设计　□图像处理/多媒体设计

□工业设计　□计算机组装与维修　□信息化与系统安全

四、您对本书的满意度：

从技术角度　□很满意　□比较满意　□一般　□较不满意　□不满意

□改进意见_____

从文字角度　□很满意　□比较满意　□一般　□较不满意　□不满意

□改进意见_____

从版面、封面设计角度　□很满意　□比较满意　□一般　□较不满意

□不满意　□改进意见_____

五、您最喜欢书中的哪篇（或章、节）？请说明理由。

六、您最不喜欢书中的哪篇（或章、节）？请说明理由。

七、什么价格的书您能接受?

☐ 30 元以下　☐ 40 元以下　☐ 50 元以下　☐ 60 元以下

☐ 100 元以下　☐ 100 元以上　☐ 其他_____

回邮地址：（请在信封上注明“书评”或者“意见调查表”）

北京市万寿路南口金家村 288 号院 华信大厦六层

电子工业出版社计算机研发部

邮编：100036

E-mail：support@fecit.com.cn

我们期待您的参与，谢谢！

飞思科技产品研发中心

译　序

安全性本身涉及的内容和范围非常广泛，从整体层次上来说，包括安全策略、安全管理、物理安全、网络安全、主机安全、应用安全、数据安全等许多领域，针对这些主题，业界已经提供了大量成熟的解决方案和最佳实践，从微观上来说，安全基础技术——密码学的发展也相当成熟。通过在以上各个层次中合理地使用密码技术，能够有效地满足绝大多数安全需求，关于这些内容的安全资料和书籍非常丰富，但是唯一令人遗憾的是，关于密码学在数据库中的应用这个领域，即数据库加密，却被很多安全专家和技术人员所忽视，很少有人去研究，因此也鲜有相关著作，其主要原因是大家一般寄希望于数据库管理系统来保护数据的安全性，但是在实际应用中，数据库管理系统所能提供的保护作用是有限的。

大多数情况下，应用系统中最有价值的资产就是商业数据，尤其对一些特定行业如金融行业来说，数据的机密至关重要，甚至事关企业的命运和发展。例如，去年美国付款信息处理公司 CardSystems 遭受黑客入侵，造成了美国史上最大一起数据泄露事件，此次泄密事件波及的信用卡用户多达 4 000 万人，严重影响了全世界范围的数千万客户，甚至包括中国的数千名用户，这使得银行和信用卡公司不得不为所有客户重新换发所有信用卡，这不但带来了巨大的业务损失，更重要的是，对公司的声誉、客户的信心带来了沉重的打击。

由此可以看出，数据安全是整个系统安全中非常重要的一个环节，虽然应用程序和数据库管理系统可以为数据提供相当大程度的安全保证，但是要看到，由于数据在物理上一般存储在单独的服务器上，攻击者可以很容易破解或绕过应用程序而直接访问数据库，另外，由于数据库管理系统使用不当或者攻击者绕过数据库管理系统来直接访问数据库所对应的原始文件，数据库管理系统所提供的安全保护也失效了，除此之外，那些合法的用户，如数据库管理员、应用开发人员都有可能轻易读取数据库中的内容，从而破坏数据的机密性。因此，如果不在数据库内部实施额外的安全措施，如数据库加密，就难以完全保证数据的安全性。

考虑到数据库系统的复杂性，因此保护数据库并对其进行加密也是一个非常错综复杂的问题，如密码算法和模式的选择、密钥的管理等，如何才能有效地入手呢？《数据库加密——最后的防线》这本来自业界领先的安全公司 Symantec IT 应用与数据库安全项目主管的著作，将带给你这些问题的答案。

在本书中，作者 Kevin Kenan 全面地介绍了与数据库加密这个主题有关的方

方面面的问题。包括解保护数据的必要性，如何构建一个真正的数据库威胁模型，加强数据库安全的需求分析、对数据进行分类、如何编写与密码系统安全交互的数据库应用程序、避免常见的威胁数据库安全的漏洞和问题，以及如何在测试、部署、保护及终止过程中保护数据库应用的安全性等。

本书分为4大部分，第1部分首先介绍了安全性的基本含义及其在数据库中的具体体现，随后讲述了密码学和数据库的一些基础知识和密码学在数据库中的应用。在第2部分中，介绍了密码系统的基础架构和密码系统中的各个组件，如密钥库、密钥管理器、密码提供者、密码引擎等。

第3部分介绍了密码系统的项目管理，描述了一个项目开发生命周期的各个阶段应该注意的安全问题，如在需求阶段进行需求定义，确定策略、标准及算法；在设计阶段，提到了应该遵循的安全设计指南及最佳实践，并介绍了威胁建模及安全模式方面的内容；在开发阶段，介绍了应该注意的最主要的安全开发实践；在测试阶段，主要介绍了安全功能测试和穿透测试，前者是从正面的角度测试各种功能是否存在，而后者是从攻击者的角度来测试系统安全措施的有效性如何，是否存在任何漏洞。最后，介绍了应用程序在部署、运行及终止阶段应该注意的安全问题，这是一部分很容易被忽视的重要内容。

在第4部分中，作者针对之前描述的各种理论、技术与实践，给出了一个数据库加密系统的Java实现，这是本书中非常有价值的一部分内容。通过这部分代码，读者可以更准确、更深入地了解本书中的内容，最后，给出了这个示例系统的运行演示。这些代码在做少量修改后，就可以应用到实际的项目中去。这部分代码可以从作者的网站（http://www.kevinkenan.com）上下载，其中包括了相关的使用说明，包括如何建立初始数据库等。

感谢本书的另两位译者马超和林滨，他们为本书的翻译工作付出了很多的心血。在本书翻译和审校过程中，我们也得到徐化冰及北京邮电大学信息安全中心胡兰兰博士的大力协助与支持，在此一并表示感谢。。

由于译者水平有限，书中内容表述难免有不妥之处，恳请读者批评指正。

李彦智

关于作者

Kevin Kenan 是 Symantec 公司 IT 应用与数据库安全项目的主管。他在这个位置上的工作是与应用开发团队一起确保 Symantec 公司内部部署的各个应用系统和数据库系统的安全性。这项工作的主要内容是制定密码系统的解决方案，从而确保所有在系统中存储的敏感数据的安全性。

在此之前，他曾在 Symantec 公司的信息安全部门工作，为 Symantec 公司的信息技术和产品开发团队设计和开发软件，这些软件大多都对安全性和加密具有很高要求。他还曾经为使用 Symantec 公司的开发工具的企业用户提供技术支持。他拥有俄勒冈大学（University of Oregon）数学科学专业的学士学位。

关于本书

这是一本关于如何使用已有的密码技术和算法对数据库中存储的信息进行保护的书。本书所关注的内容主要是如何设计、建立（或者挑选、集成）一套密码系统，以用来保护数据库系统，并防范那些被明确确定的威胁。在本书中，假设安全性在系统中的优先级是最高的，因此本书中不仅讨论了数据加密问题，还讨论了如何防止针对加密数据发动的攻击。

如果在实现密码系统时稍有不慎，那么即便对数据进行了强加密保护，攻击者也还是可以破解数据。在安全通信领域可以见到很多这样的例子。例如，无线加密协议 WEP（Wired Equivalent Privacy，有线等效加密）中存在广为人知的缺陷，虽然这些缺陷在 WPA（Wireless Protected Access，无线保护访问）中得到了很大改进，但代价却是用户需要购买新的设备。在数据库加密系统中，也可能存在这种带来致命危害的缺陷。一般的简单加密对于数据保护来说是不够的。在本书中，我的目标是给出一个切实可行的蓝图和执行计划，以便项目团队能够成功地完成加密保护数据库中的敏感信息的任务。

本书中描述的密码系统可以被当做一个原型，在这个原型中，指出了系统中存储的数据所面临的威胁，并且说明了如何对这些威胁进行防范。在实施密码系

统的过程中，可能会遇到各种问题和常见失误，例如，如何选择加密模式和如何管理密钥等，这些问题在书中都已被明确指出并提供了解决方案。这个密码系统的架构是灵活的，可以适应多种环境的要求。

当书中给出的解决方案不能满足实际情况的要求时，首先，应该要获取足够的相关信息和指南，然后对设计进行修改。同样，当你在对厂商提供的数据库密码系统进行评估时，可以使用本书中讲述的系统设计作为基线与之进行对比，然后再做出决策。

即使这些厂商提供的密码系统与书中的设计有着很大的差异，但是这些系统也还是需要将密钥分配给数据表的行和列，还是会有密钥生命周期的。此外，它也需要存储并保护密钥、需要合理的加密模式、需要处理初始化向量等。最重要的是，任何解决方案的目标都是最大限度地降低公司威胁模型中所列出的风险。你必须考虑到所有这些细节。本书讨论了这些问题并且提供了一个可以运行的密码系统，希望这本书可以帮助项目团队成功地构建或购买一个数据库密码系统。

本书的读者对象

本书面向的最主要的读者是那些负责保护数据库中敏感信息安全的技术主管。他可以是一名架构设计师、资深系统分析人员或安全分析人员、数据库管理员或技术项目经理等。一个成功的项目要求项目团队能够正确地、安全地实施密码系统的架构，所以在整个项目的开发过程中，安全技术主管必须要给大家提供安全开发技术和实践。

本书假设技术主管是一个资深的应用安全分析人员。开发团队的责任是负责实现一个处理并存储敏感数据的应用系统，我们的分析人员也是这个团队中的一员。分析人员的第一项工作是帮助项目团队、管理层和客户意识到加密是十分必要的，然后，分析人员将投入到项目团队的各个阶段的工作中，确保密码系统的需求定义、设计和实现过程都是正确的、安全的。

如果项目团队中没有专门的安全分析人员，那么团队中的其他角色，如系统架构师或者系统分析人员可以负责这部分工作，直到与系统安全有关的问题被明确之前，这都是他的一个核心职责。在有些项目中，安全分析人员的工作可以分给多个人来完成，合理的划分方法是一个人作为主要关注安全问题的技术指导，

如系统架构师，而另一个人作为项目经理。

读者的背景要求

本书假设读者熟悉数据库，并且具备密码学方面的基本知识。在深入探讨数据库和密码技术之前，本书会对这些知识进行简要的复习。要想阅读本书后面的示例代码，读者需要有 Java 或其他编程语言方面的经验。同样，应用系统开发方法论方面的知识对于帮助理解安全开发实践相关的问题是很有帮助的。

本书的内容组织

本书分为 4 部分。第 1 部分概括地讨论了数据库安全问题；第 2 部分详细地讨论了数据库密码系统的设计；第 3 部分讨论了安全地实施密码系统所必需的开发过程；最后一部分提供了按照之前的设计实现的示例代码。

在第 1 部分“数据库安全”中，第 1 章中讨论了为什么数据库安全如此重要，同时也讨论了数据库面临的各种攻击。讨论的结果就是总结了数据库安全的威胁模型。本章也对各种与数据库安全有关的法规做了简要的介绍。第 2 章讨论了密码系统可以为数据库提供哪些类型的保护，本章也阐述了密码系统本身也会引发新的风险，为进一步检查密码系统的弱点做了准备。我们不能假定数据被加密后就安全了，即使是使用了强加密算法。

第 2 部分“密码基础设施”详细地说明了如何进行密码基础设施的设计。第 3 章对密码系统进行了概述，并且介绍了如何进行密钥管理，如何使用密钥来对数据加密。第 4 章介绍了密码算法和密码引擎。密码引擎是具体进行密码操作（加解密操作）的组件。本章讨论了多种不同种类的引擎。本书中示例程序所使用的密码算法（即 AES）有好几种应用模式，本章讨论了这些模式，并且也考虑了错误地使用模式时会引入的漏洞。第 5 章介绍了存储和管理密钥的组件。第 6 章描述了应用程序是如何与密码系统进行交互的。

第 3 部分为“密码项目”，乍一看似乎有点离题，因为这一部分主要关注的是安全开发实践。如果你是安全应用程序开发方面的专家，你可以复习一下这 6 章内容，但是经验显示（这并不是指那些在每周新闻中报道的安全攻击行为），安全

开发方面的专业知识还不够普及。数据库加密系统是一家公司安全基础设施的一个主要部分，其他应用的安全都依赖于密码系统的安全性，所以要尽一切努力去保证实现过程的安全。数据库加密系统中的漏洞会使整个公司中的数据面临极大的风险，因此突出这个主题是很必要的。

从第 7 章开始，我们开始讨论安全开发实践，在第 8 章中，说明了如何挖掘安全与加密需求，同时也讨论了数据的类别划分。第 9 章的主题是如何保证设计本身的安全性，其中讲述了设计指南、威胁建模和应用系统的安全模式等。第 10 章给出安全编程（大多数人把它看做是开发）的通用指南。最后两章，即第 11 章和第 12 章讲述了系统的测试、部署、保护和停止运行等内容。

第 4 部分“示例程序”由代码和相关注释组成。第 2 部分中讨论的各个组件和几乎所有核心功能都在这里实现了。这些代码可以帮助你研究和体验一下一个能够真正运行的数据库加密系统。希望这些真正的示例程序能够帮助你更加清晰地了解之前各章节所介绍的理论内容，同时也希望它能帮助你实现或评估一个能够投入生产的密码系统。在第 21 章中，演示了示例系统的实际运行情况，其中包含从设置密钥加密到查询加密数据等各个功能。

作者

目　录

第 1 部分

数据库安全

- 数据库安全问题
- 利用密码技术保护数据库