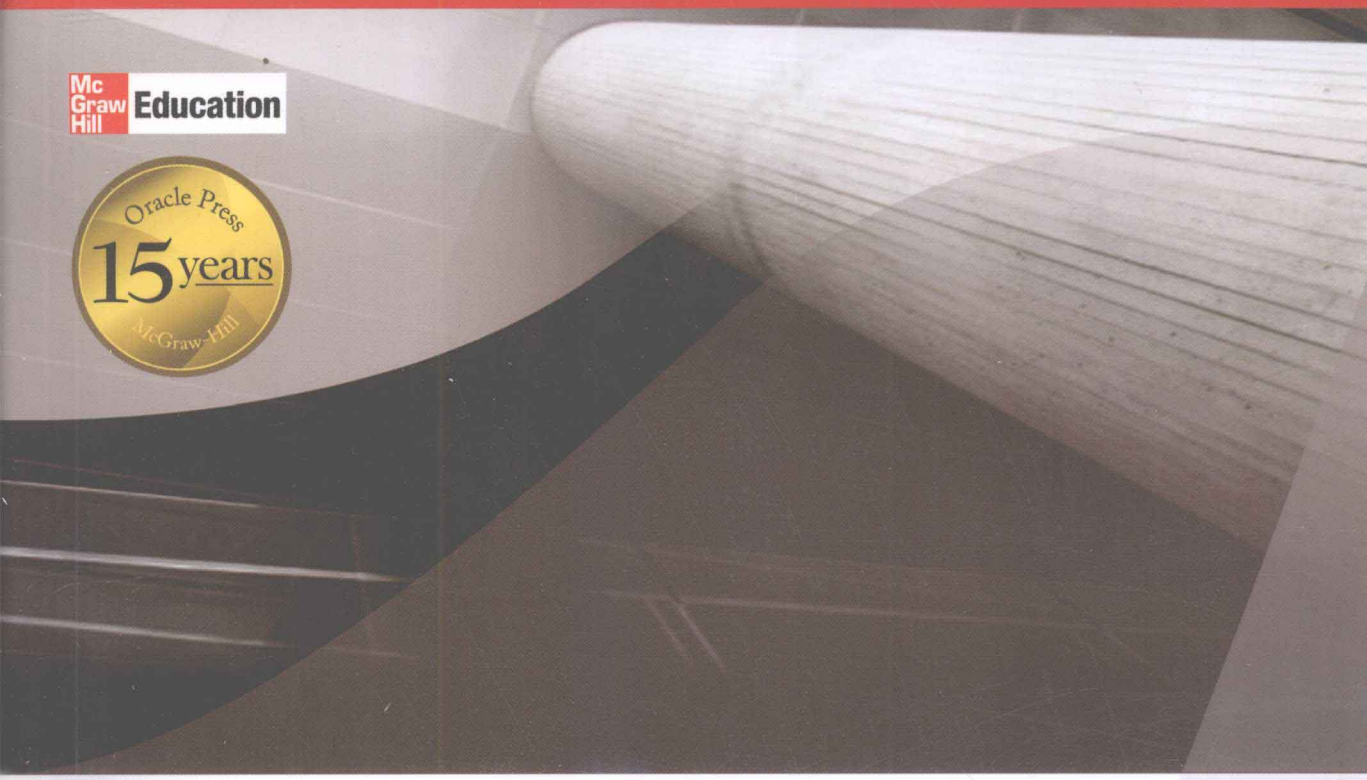
ORACLE



Applied Oracle Security: Developing Secure Database and Middleware Environments

ORACLE DATABASE

ORACLE FUSION MIDDLEWARE

Oracle安全实战

——开发安全 间件环境

Oracle公司首席架构师Edward Screven作序推荐

(美) David C. Knox
Scott G. Gaetjen 等著
孟祥旭 唐扬斌 译

ORIGINAL • AUTHENTIC
Oracle Press
ONLY FROM OSBORNE

清华大学出版社

Oracle 安全实战——开发安全的数据库与中间件环境

(美) David C. Knox
Scott G. Gaetjen 等著

孟祥旭 唐扬斌 译

清华大学出版社

北 京

David C. Knox, Scott G. Gaetjen, et al.
Applied Oracle Security: Developing Secure Database and Middleware Environments
EISBN: 978-0-07-161370-5

图书在版编目(CIP)数据

Oracle 安全实战——开发安全的数据库与中间件环境/(美)诺克斯(Knox, D.C.)，(美)格特延(Gaetjen, S.G.) 等著；孟祥旭，唐扬斌 译. —北京：清华大学出版社，2011.7

书名原文：Applied Oracle Security: Developing Secure Database and Middleware Environments

ISBN 978-7-302-25632-8

Ⅰ. O…　Ⅱ. ①诺… ②格… ③孟… ④唐…　Ⅲ. 关系数据库—数据库管理系统，Oracle—安全技术

Ⅳ. TP311.138

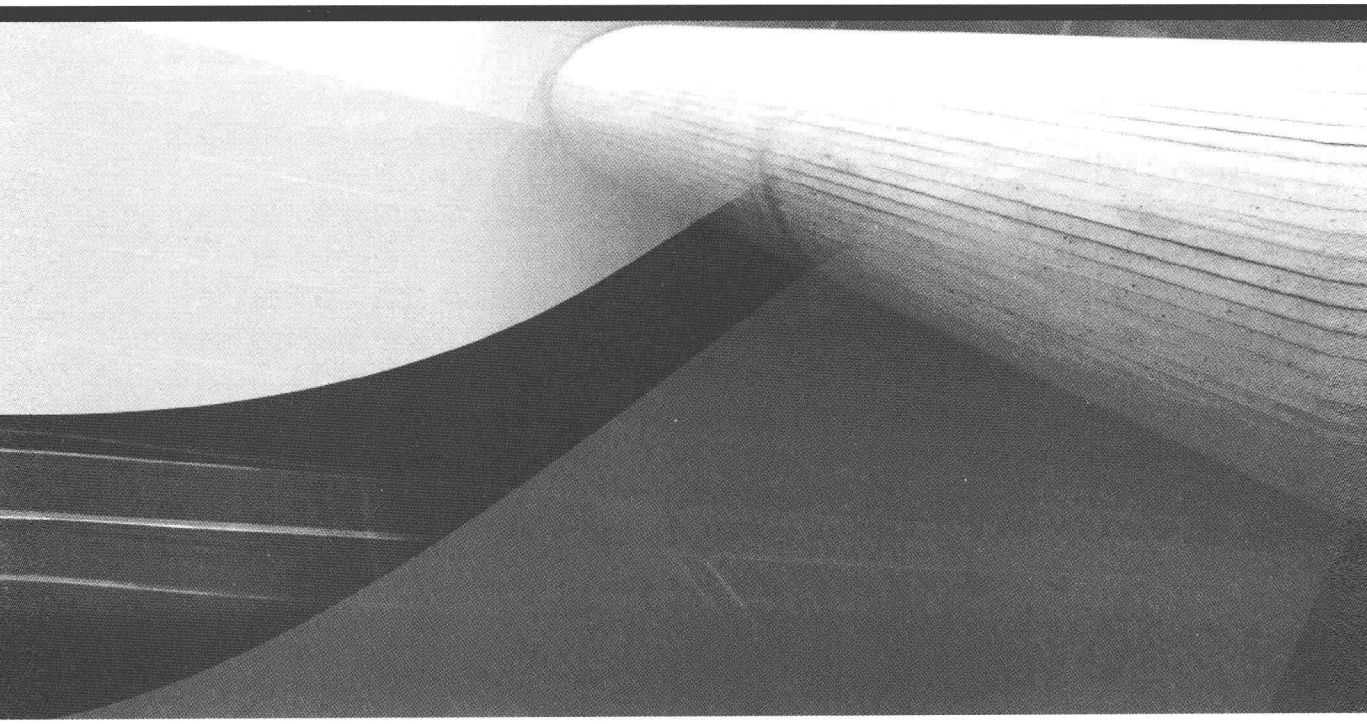
中国版本图书馆 CIP 数据核字(2011)第 096077 号

责任编辑：王　军　于　平
装帧设计：孔祥丰
责任校对：胡雁翎
责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：36.75　**字　数**：941 千字
版　　次：2011 年 7 月第 1 版　　**印　　次**：2011 年 7 月第1 次印刷
印　　数：1～4000
定　　价：69.00 元

产品编号：032200-01



译 者 序

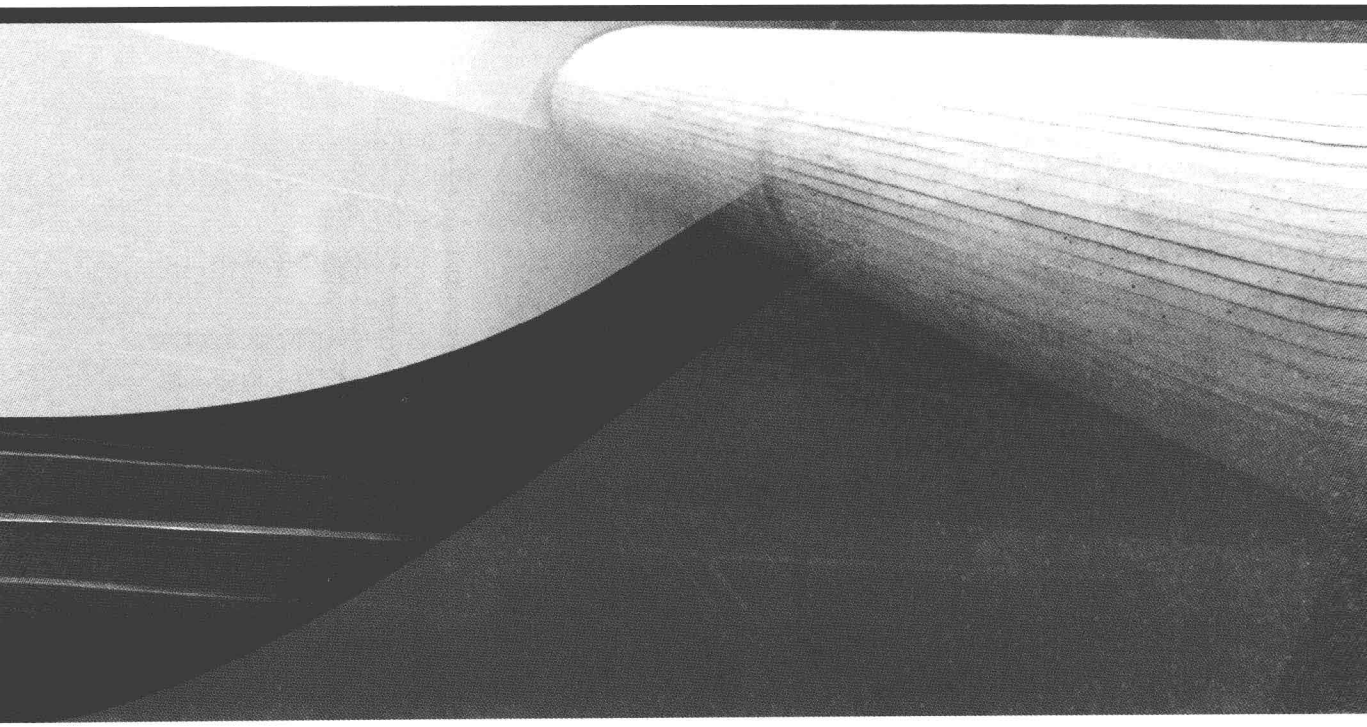
本书是 David C. Knox 继 *Effective Oracle Database 10g Security By Design*(McGraw-Hill 出版社 2004 年出版)之后的又一力作，得到了 Oracle 官方技术网站 OTN(Oracle Technology Network)的极力推荐。所有作者都是来自 Oracle 内部的资深研发和工程人员，很多人曾经是 Oracle Database Vault 等杰出的安全产品研发团队中的成员。他们对于 Oracle 的安全机制如数家珍，讲解起来可以追根溯源、深入浅出，对于很多关键机制的讲解更会使您有醍醐灌顶之感。整本书围绕几个简单的安全实例(基于 Oracle 示例数据库)展开，将各种安全机制和技术融入其中，相互辅衬，前后关联。认真读来，可以更深入地理解如何灵活自如地运用 Oracle 安全机制。

随着社会的进步，敏感数据越来越多，人们更加关注自己的隐私问题，各种法律法规对企业数据操作的监管也越来越严格。在这样的背景下，Oracle 的安全研发人员一直努力在完善自己的安全机制：为了解决特权账户带来的风险，防范内部人员的攻击，研发了 Oracle Database Vault；为了符合新的法律规定，设计实现了更加先进的身份管理策略和细粒度的审计策略。可以说 Oracle 一直在坚持不懈地努力，尽其所能帮助客户解决安全隐患。而本书无疑是对 11*g* 中新的安全特性的最权威解读。同时，在您企业的信息系统中，使用 Oracle 提供的最新安全防护机制是保护敏感数据的最有效途径。

本书是一本理论性和实践性都很强的书，因为作者相信“您对安全组件的架构和原理了解得越多，就越能够有效地降低安全风险”。所以在使用本书时，要先从宏观上掌握 Oracle 安全体系的整体脉络和原理。如孔子所言“学而不思则罔，思而不学则殆”，在阅读本书的时候，也要“读”“思”并举，尤其要积极思索各种技术的动机和用途，深入理解作者提出的种种安全原理，并将各个分散的部分在头脑中组建成一个有机整体。

“实践出真知”，建议您在阅读的过程中也不断地动手实践，对书中的实例亲自调试运行，最好能够结合自己的工作，做到举一反三，灵活运用。

本书由孟祥旭和唐扬斌翻译。敬请广大读者提供反馈意见，读者可以将意见发到 wkservice@vip.163.com，我们会仔细查阅读者发来的每一封邮件，以求进一步提高今后译著的质量。由于译者水平有限，时间紧迫，故译文中必定存在很多不足之处，希望读者能够谅解，并不吝斧正。真心希望我们的工作能够给您的工作和学习带来帮助，也希望通过您的安全实践给社会带来更多的安全收益！



作者简介

David C. Knox，Oracle 公司解决方案工程部门的高级经理，现担任 Oracle National Security Group 高级经理。从事该工作之前，曾担任 Oracle 北美分部销售和咨询解决方案工程师，得以了解 Oracle 技术体系内部关于解决方案和 R&D 创新的方方面面。还曾担任 Oracle Protected Enterprise & Security Business 的高级经理及 Oracle Information Assurance Center 的主任工程师。

自 1995 年加入 Oracle 起，Knox 曾与许多客户组织一起开展工作，包括美国国防部、CIA、商务部以及其他许多工商业机构，这使他对关键商业驱动力及其实现过程有着非常广泛而深入的了解。他在计算机安全领域的专家身份不仅源于他对 Oracle 安全产品和数据库安全技术的全面理解和丰富经验，也源自他作为一位学者对多层次安全、密码学、LDAP 及 PKI 等理论与技术的深入研究。

Knox 是 *Effective Oracle Database 10g Security By Design*(McGraw-Hill 出版社 2004 年出版)一书的作者。此外，他在安全领域的著作还包括：Thomas Kyte 主编的 *Expert One on One Oracle*(Wrox 出版社 2001 年出版)以及 *Mastering Oracle PL/SQL: Practical Solutions* (Apress 出版社 2003 年出版)。他参与编著了多本 Oracle 技术白皮书。Knox 拥有 University of Maryland 的计算机科学学士学位和 Johns Hopkins University 的计算机科学硕士学位。

Scott G. Gaetjen，技术经理，Oracle National Security Group，主要从事安全解决方案的

设计与开发，他以在 Oracle 技术部门 15 年的工作经验，致力于为客户提供更先进的安全防护能力。作为技术负责人和导师参与了众多客户的项目，包括美国国防部、CIA、国土安全部、国民政府和其他金融工业机构等。帮助这些客户实现追求的任务目标的过程，使他能够深入理解操作系统安全、Oracle 数据库安全、J2EE 安全和身份管理等技术。

自 Oracle Database Vault 项目 2004 启动，Gaetjen 就开始参与其研发工作。该产品最终由 Oracle 咨询部门的一个解决方案发展成为了一项独立而强大的 Oracle 软件产品。

Gaetjen 拥有 James Madison University 的数学学士学位以及 University of Maryland University College 的计算机系统管理硕士学位。

Hamza Jahangir 目前担任 Oracle Enterprise Architecture 工作组的主任架构师。他于 2004 年加入 Oracle 公司，已经从事 Oracle 数据库和中间件方面的工作 10 余年。作为架构师，他花费了大量时间为客户提供技术指导，帮助客户更好地理解和应用各种安全产品与技术，以应对来自数据库和中间件领域的各种挑战(如身份管理、访问控制、目录与 J2EE 安全)。

Jahangir 同时还教授安全方面的课程，并且花费很多时间致力于数据库与中间件安全技术的结合，并最终为 Oracle 的用户群体和专业人士提供围绕身份管理、面向服务的架构和 IT 安全方面的支持。此外，他剩余的工作精力主要放在了与企业安全模型相关的新体系结构与解决方案原型的实验上。

如果不工作，他喜欢和家人、朋友以及自己那把传统的尼龙琴弦的吉他呆在一起。他拥有 Northeastern 的计算机科学学士学位，目前正在攻读 Georgetown 的 MBA。

Tyler Muth 是 Public Sector division 的主要技术人员之一。他在美国境内开办了许多 APEX 讨论班，为客户提供体系结构方面的建议，并与他们合作开发应用程序。在 Oracle Technology Days、Oracle User Groups 和他的博客 www.tylermuth.wordpress.com 中，可以看到大量由他提供的讲座。在 Oracle Technology Network 论坛上也不乏他的身影。

在担任现在角色前，Muth 是 APEX 开发小组的早期开发者之一，他在那里工作了 5 年多。他还担任了 Tom Kyte 多部技术书籍的技术审稿人，Tom kyte 是 asktom.oracle.com 的主要参与作者，以及零重力生产系统的经理。

Patrick Sack，技术副总裁，NSG Product Engineering，负责 Oracle National Security Group 的 Product Engineering 分部。从事这一工作前，曾任 Oracle Protected Enterprise & Security Business 部门的副总裁。职业生涯的大部分时间都在 Oracle Consulting 集团中度过，期间为推动 Oracle 产品的创新发挥了巨大作用。

在 1988 年加入 Oracle 前，Sack 与许多客户组织一起工作过，包括美国国防部、CIA、商务部及其他许多的工业界组织机构。这使他对关键业务驱动力和过程有着非常广泛的了解。他在信息安全方面的专长源自对 Oracle 产品的丰富知识，以及参与过的众多客户项目，包括多层次的安全技术。

Sack 是 Oracle Information Assurance 技术、体系结构和解决方案方面的专家。他曾致力于为客户定制新的安全技术、特性和完整的解决方案，其中就包含用于遵从性的 Database Vault 技术。他是 Oracle 数据库产品中许多新安全特性的主要发起人，如 Oracle Database Vault、Oracle Audit Vault、Oracle Label Security 及细粒度的审计。在 Oracle 公司的美国专利注册中，经常能够看到他的名字，这些专利包括：多数据库安全政策、原级审计、Database Vault、

Mandatory Access Control Base、Dynamic Access Controls 以及审计和跨域安全等。

Sack 了解对于大多数组织机构而言，什么才是关键信息以及相关的安全问题，因此他始终强调数据的可用性、可追溯性和可达性。他拥有 State University of New York 的计算机科学学士学位。

Richard Wark，CISSP，Oracle Enterprise Solutions Group 的主要技术工程师之一，自 2004 年开始协助开发安全和身份管理的解决方案、演示以及培训系统。2002 至 2003 年间，他主要为圣安东尼奥市工作，协助管理一个大型的 ERP 项目。1996 年刚加入 Oracle 时，他是负责全国范围内空军客户的销售顾问。此后，他先后参与了包括银行、航空公司、金融机构和其他许多公司机构的数据安全项目。

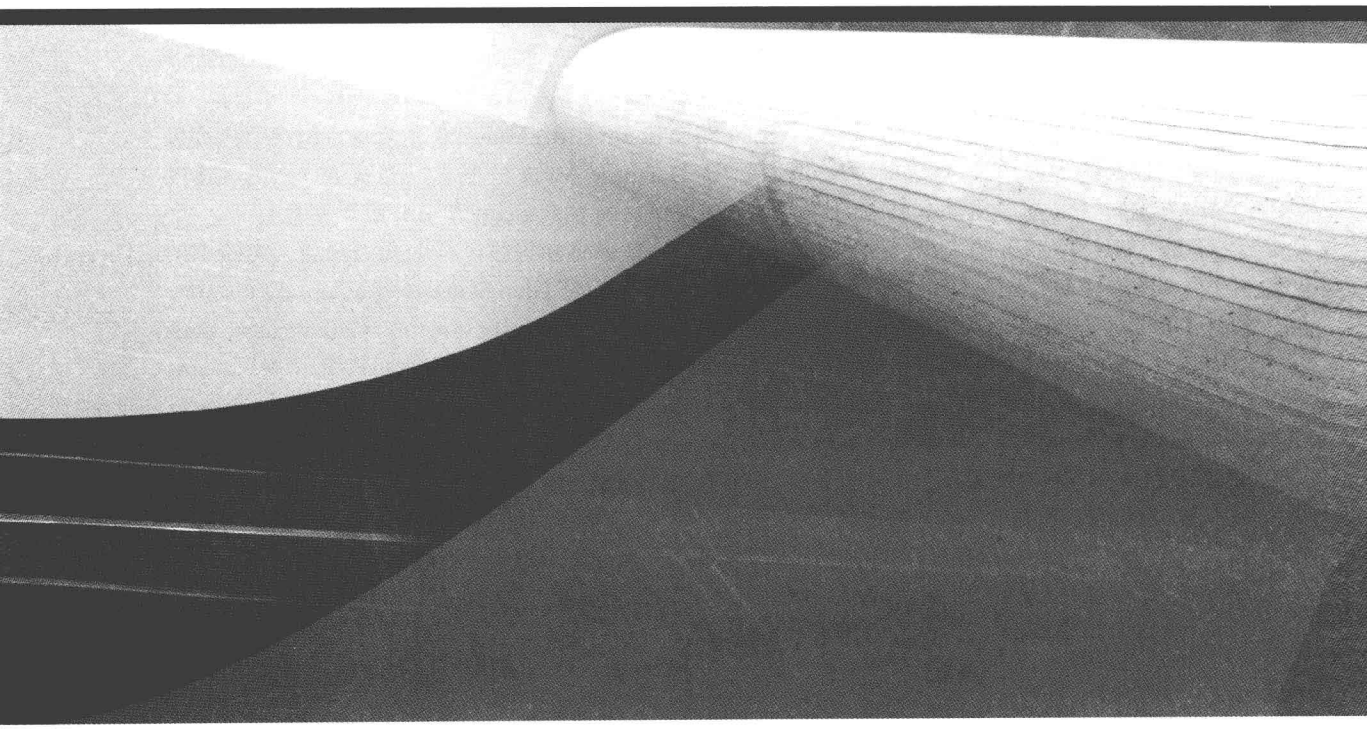
在超过 15 年的 Oracle 产品生涯中，Wark 参与过美国政府，以及美国国防部、医疗卫生行业和其他商业组织的数据安全项目。通过不断挑战新的问题，他积累了非常丰富的知识和实践经验，成为了网络安全设计、安全政策创建、业务连续性规划、数据分类、安全数据库配置和大规模实现方面的专家。

加入 Oracle 前，Wark 曾为 Computer Sciences Corporation(CSC)和 Science Applications International Corporation(SAIC)工作，主要从事美国国防部的 Oracle 数据库项目。他的职业生涯的起点是 1991 年，当时他是一名 UNIX 管理员和 Informix 的 DBA。他拥有 University of Texas(San Antonio)的信息系统学士学位。

Bryan Wise 是 Oracle Public Sector 部门的 BI 解决方案专家，其职责是寻找安全和具有创造性的途径帮助组织机构更好地使用所拥有的数据。他 20 世纪 90 年代末加入 Oracle，此前曾服务于美国海军，负责管理所有的数据库，并领导海军核动力学院的应用程序开发和报表工作。

多年来，Wise 积极参与了 Oracle 社区的活动，在 Mid Atlantic Association of Oracle Professionals、Oracle Government Users Group 和 IOUG 的 Business Intelligence, Warehousing and Analytics Special Interest Group 都可以看到他做过的报告。同时，他也是 Oracle BI Publisher 博客的主要作者之一。

除了作为一名 Oracle 技术专家，Wise 将许多时间用于教学，包括开办 Oracle Business Intelligence 的讲习班、在海军核动力学院教授数学课程以及在 University of Maryland University College 教授数据库课程。他拥有 Brigham Young University 的数学学士学位以及 Regis University 的电子商务工程硕士证书。



致　谢

我首先要感谢为本书的诞生而辛勤工作的优秀作者团队，其中每一位都拥有关于本领域难以被超越的专业知识。尽管我写过关于 Oracle 安全的书，但我坚信本书汇集了关于 Oracle 安全技术的最佳实践、概念、思想和建议。我认识到说“我在写一本书”和实际写一本书之间的巨大差别，在此我要真心地感谢本书团队自始至终的努力，我们不仅顺利完成了本书，而且完成得非常出色。感谢 Richard、Pad、Scott、Hamza、Tyler 和 Bryan，感谢你们的坚持不懈和不辞辛劳的工作。

我还要感谢我在 Oracle 的同事和 Oracle 的管理团队。编写本书并不是我的本职工作，感谢他们的巨大支持和鼓励，使我能够获取可用于整个 Oracle 社区的信息。Mark Tatum 和 Glen Dodson 给了我特殊的帮助，而没有 Edward Screven 的支持，本书不可能最终完成。我的团队伙伴——Ed Montes、Fred Justice、Joe Mazzafro 和 Mark Lunny——在本书的编写过程中一直和我并肩战斗。我要感谢 Vipin Samar 和 Paul Needham 的团队，多年来给予我巨大的支持。Tammy Bednar 则在本书编写的过程中扮演了重要的角色。

最后，我想感谢我的太太 Sandy，以及我的孩子们。Sandy，你再一次给予我这样多的时间和空间(来写这本书)，而我曾经说过再也不会这样了。我能感受到你的牺牲，我明白没有你的支持这一切不可能完成。对于孩子们，我想说真的对不起，在编写本书的过程中没有太多的时间来陪伴你们。我希望你们能明白，虽然爸爸有时候不得不投身辛勤的工作，但在我的心中，你们才是最重要的。我爱你们！现在开始，我们又可以一起捉迷藏了，准备好了吗？

——David Knox

Patrick Sack 想感谢 Glen Dodson 和 Ray Prescott，他们提供了非常具有创造性的环境，这样的环境为各种新想法提供了诞生的土壤，并使这些想法不断发展完善，最终成为具有商业价值的解决方案所需的文化。谢谢你们，Glen 和 Ray。

Patrick Sack 还要特别感谢 Scott Gaetjen 和 William (Bill) Maroulis 的睿智、积极的态度以及非常投入的专业精神。Scott 和 William 围绕 Database Vault 的概念，开发了一系列关键的解决方案，并最终启发了本书中的许多概念和案例。特别向 Scott 和 Bill 致以谢意！

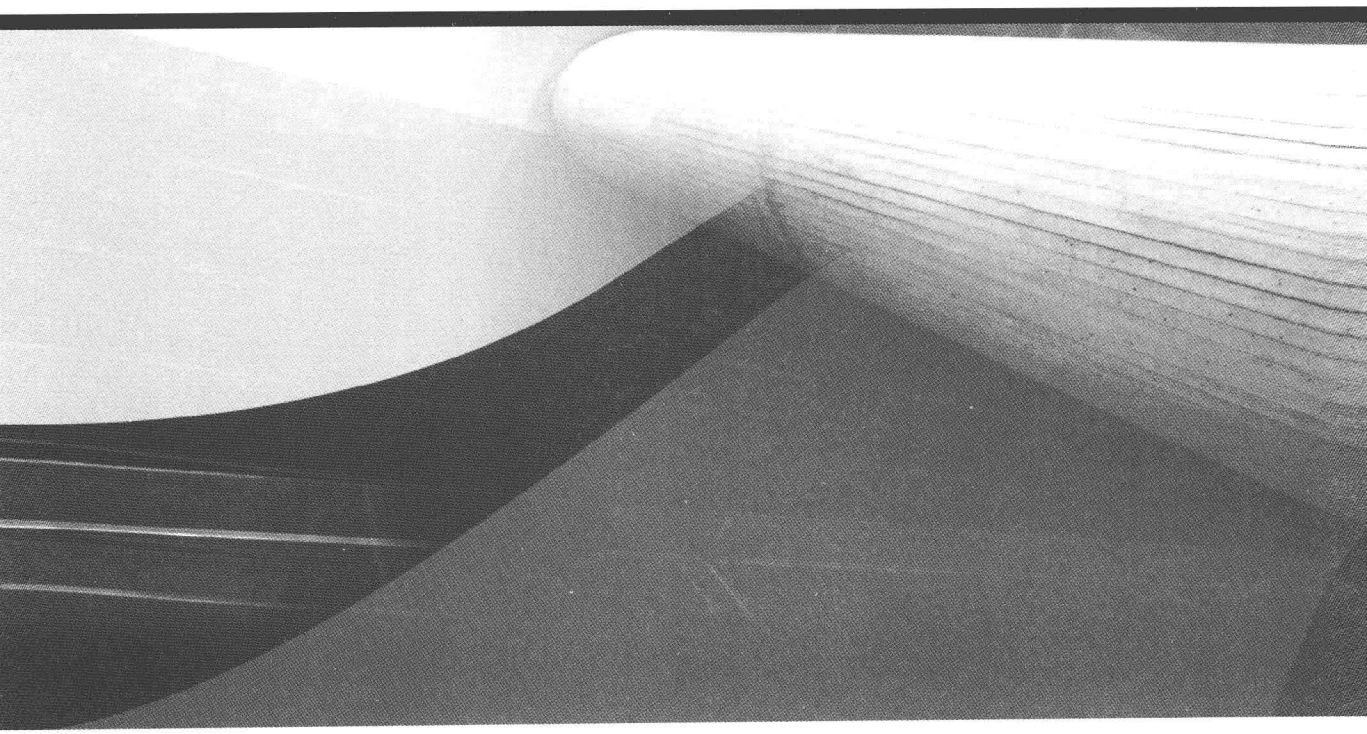
我们想感谢如下的人士，他们为本书提供了许多灵感和思路，帮助我们扫清了道路上的障碍，最终使 Database Vault 成为一个成熟的产品，他们是 Glen Dodson、Raymond Prescott、Jay Gladney、Jon Bakke、Wendy Delmolino、David Knox、Rusty Austin、Gail Wright、Jack Brinson、Chi Ching Chui(以及他的团队)、Chon Lei、Ben Chang、Vipin Samar、Paul Needham、Daniel Wong、Kamal Tbeileh、Aravind Yalamanchi、Timothy Chorma、Frank Lee、Nina Lewis、Maria Chen、Cindy Li、Matthew Mckerley、Xiaofang Wang、Martin Widjaja、Sumit Jeloka、Patricia Huey、Ernest Chen、James Spiller、Tom Best、Duncan Harris、Howard Smith、Andy Webber 和 Jeff Schaumuller。

我们还想感谢 Oracle NSG(National Security Group，国家安全工作组)的销售和咨询团队，以及 Oracle Database Security(数据库安全)开发团队。正是 Oracle 中的这些工作组共同努力，才将业界最好的安全产品和解决方案呈现在信息技术领域最需要这些技术的客户面前。

——Patrick Sack 与 Scott Gaetjen

我想感谢所有和我一起工作的伙伴，因为他们的辛勤工作才使得本书最终诞生。特别感谢 David Knox 的指导和一直以来的支持与陪伴。还要感谢 Richard Wark、Pat Davies、Al Kiessel、Matt Piermarini 和 Colin Nurse 方方面面的支持与帮助。最后，感谢我的两位同胞，Javed 与 Tabassum，他们始终如一的支持是我前进的动力。感谢你们的爱、关心与陪伴。

——Hamza Jahangir



序　言

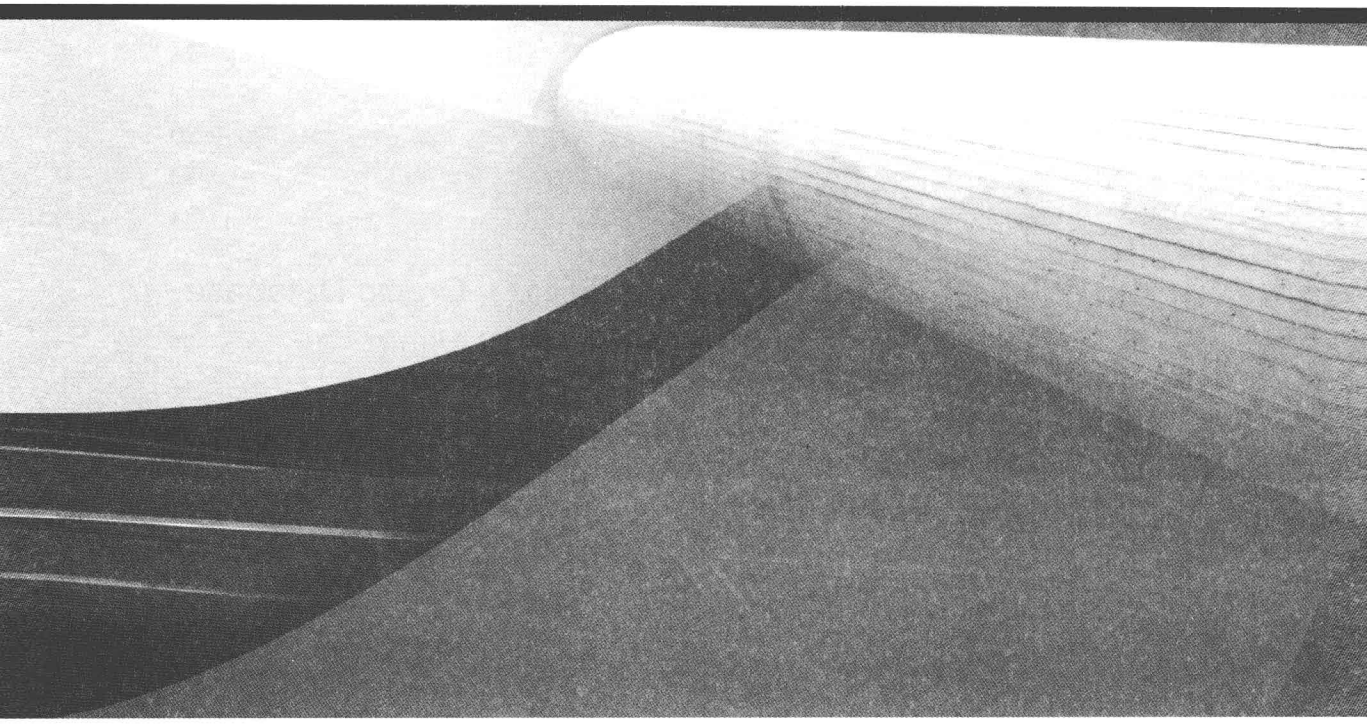
Oracle 业务的核心是信息：信息的管理、信息的利用及信息安全。作为 Oracle 的首席架构师，我不仅仅要确保我们的技术能够为客户创造价值，还包括使之以可靠的方式实现。在我经历过的每一次对客户经理的访问中，都会谈及安全问题，因为其重要性毋庸置疑。今天，安全、隐私及信息的监管对每个人来说都是最重要的事情。对于每个人，它们早已不是“锦上添花”的奢侈品，而是“不可或缺”的实际需求。正因为如此，人们一直都在努力寻找各种途径，确保自己已经完成了满足这些需求所需完成的任务。

本书讲解了从体系结构、设计场景到 Oracle 编码配置等多方面的内容，其目的是帮助 Oracle 客户实现可靠的信息安全系统。本书最引人注目之处在于它完全由 Oracle 内部的专家编写。几位作者都是每天为实际客户寻求安全方案的顶尖工程师。Oracle 的许多产品和技术正是诞生于在这些专家与一线客户实际接触所积累下的丰富经验之上的。

毫无疑问，您一定会在本书中找到非常深入和有价值的信息。建议您从头开始仔细地阅读本书，及时在重要的地方做好书签，当然，最重要的，应该是亲自动手，将其中的方法和建议付诸实践。

——Edward Screven

Oracle 公司首席架构师



目　录