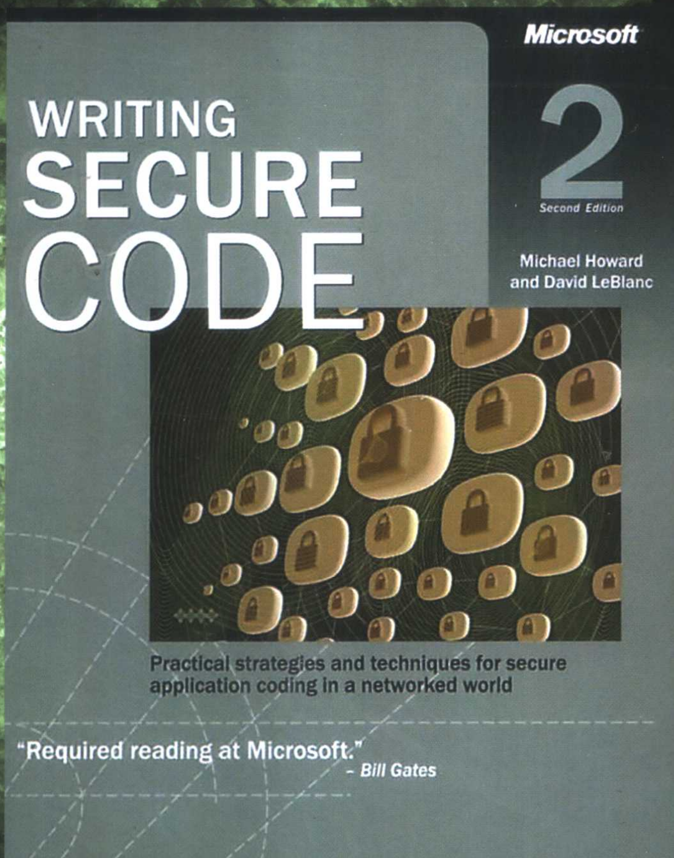
Microsoft Press 计 算 机 科 学 丛 书

第2版

编写安全的代码

(美) Michael Howard David LeBlanc 著 程永敬 翁海燕 朱涛江 等译



Writing Secure Code

Second Edition

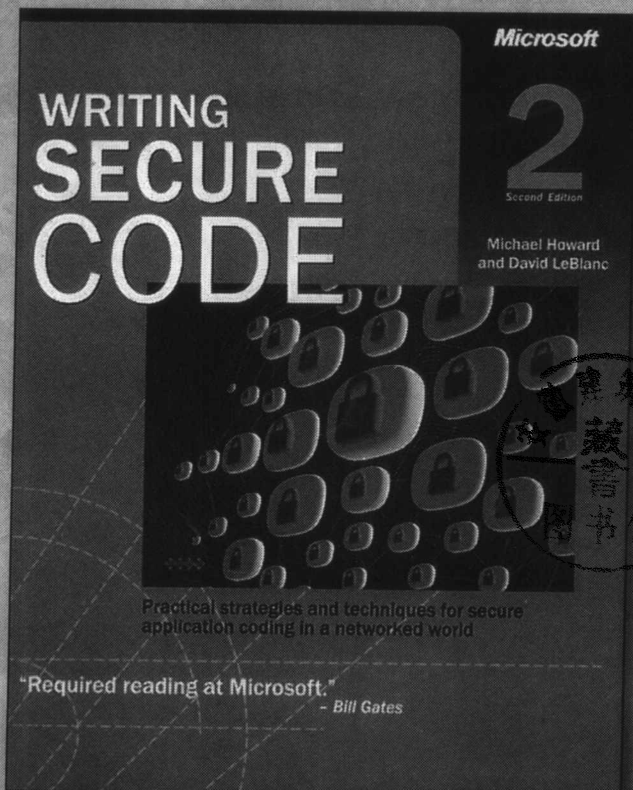
机械工业出版社
China Machine Press

计算机科学丛书

第2版

编写安全的代码

（美）Michael Howard David LeBlanc 著 程永敬 翁海燕 朱涛江 等译



Writing Secure Code
Second Edition

机械工业出版社
China Machine Press

本书分为五部分。第一部分概括说明了保护系统安全的意义，以及设计安全系统的原则和所采用的技术；第二部分概括介绍了几乎适用于任何应用程序的重要编码技术；第三部分重点介绍了网络应用程序和.Net代码安全；第四部分讨论的安全问题在一般图书中少有论及，如测试、进行安全代码审查、隐私策略以及安全的软件安装等问题；第五部分是附录，分别介绍危险的API以及分别适用于设计人员、开发人员和测试人员的安全措施核对清单。

本书第1版曾作为Windows开发组全体成员的必读教材，而第2版更是总结了在针对微软产品的多次安全活动中的许多新发现。本书曾被比尔·盖茨指定为微软员工必读书籍，是软件设计、开发、测试、系统管理等人员必读的优秀教材。

本书版权登记号：图字：01-2004-5741

图书在版编目（CIP）数据

编写安全的代码（第2版）/（美）霍华德（Howard, M.），（美）莱布兰克（LeBlanc, D.）著；程永敬等译. －北京：机械工业出版社，2005.1
（计算机科学丛书）
书名原文：Writing Secure Code, Second Edition
ISBN 7-111-11210-5

Ⅰ.编… Ⅱ.①霍… ②莱… ③程… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字（2004）第100858号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：刘 晖 刘立卿
北京中兴印刷有限公司印刷·新华书店北京发行所发行
2005年1月第2版第1次印刷
787mm × 1092mm 1/16 · 31.25印张
印数：0 001 - 5 000册
定价：55.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：(010) 68326294

出版者的话

文艺复兴以降，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的传统，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭橥了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短、从业人员较少的现状下，美国等发达国家在其计算机科学发展的几十年间积淀的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章图文信息有限公司较早意识到“出版要为教育服务”。自1998年开始，华章公司就将工作重点放在了遴选、移译国外优秀教材上。经过几年的不懈努力，我们与Prentice Hall，Addison-Wesley，McGraw-Hill，Morgan Kaufmann等世界著名出版公司建立了良好的合作关系，从它们现有的数百种教材中甄选出Tanenbaum，Stroustrup，Kernighan，Jim Gray等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及庋藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力襄助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专诚为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍，为进一步推广与发展打下了坚实的基础。

随着学科建设的初步完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都步入一个新的阶段。为此，华章公司将加大引进教材的力度，在“华章教育”的总规划之下出版三个系列的计算机教材：除“计算机科学丛书”之外，对影印版的教材，则单独开辟出“经典原版书库”；同时，引进全美通行的教学辅导书“Schaum's Outlines”系列组成“全美经典学习指导系列”。为了保证这三套丛书的权威性，同时也为了更好地为学校和老师们服务，华章公司聘请了中国科学院、北京大学、清华大学、国防科技大学、复旦大学、上海交通大学、南京大学、浙江大学、中国科技大学、哈尔滨工业大学、西安交通大学、中国人民大学、北京航空航天大学、北京邮电大学、中山大学、解放军理工大学、郑州大学、湖北工学院、中国国家信息安全测评认证中心等国内重点大学和科研机构在计算机的各个领域的著名学者组成“专家指导委员会”，为我们提供选题意见和出版监督。

这三套丛书是响应教育部提出的使用外版教材的号召，为国内高校的计算机及相关专业

的教学度身订造的。其中许多教材均已为M. I. T.，Stanford，U.C. Berkeley，C. M. U. 等世界名牌大学所采用。不仅涵盖了程序设计、数据结构、操作系统、计算机体系结构、数据库、编译原理、软件工程、图形学、通信与网络、离散数学等国内大学计算机专业普遍开设的核心课程，而且各具特色——有的出自语言设计者之手、有的历经三十年而不衰、有的已被全世界的几百所高校采用。在这些圆熟通博的名师大作的指引之下，读者必将在计算机科学的宫殿中由登堂而入室。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证，但我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。教材的出版只是我们的后续服务的起点。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

电子邮件：hzedu@hzbook.com
联系电话：(010) 68995264
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

专家指导委员会

（按姓氏笔画顺序）

秘　书　组

前　言

在2002年2、3月份，人们都顾不上考虑Windows所有正常的安全特性了。在此期间，整个开发组的注意力都转向了如何提高此产品的下一版本——Windows Server 2003——的安全上。众所周知，“安全Windows倡议”的目的是使开发组成员了解最新的安全编码技术，从而找出设计缺陷、代码缺陷，改进测试代码和文档。在此期间，本书的第1版是Windows开发组全体成员的必读教材，而第2版收录了在这场活动中以及在针对微软其他产品的后续安全活动中的许多新发现，这些产品包括SQL Server、Office、Exchange、Systems Management Server、Visual Studio .NET、.NET公共语言运行库，等等。

Windows安全活动（以及许多其他的安全活动）的出发点，源于比尔·盖茨2002年1月15日发表的“可信计算”备忘录，其中概括说明了一种高级策略，即如何向用户提交更安全、更可靠的新型计算机系统。自从有了那个备忘录，我们已经与数千名开发人员交谈、合作过，而他们异口同声地说：“我们要做正确的事情……我们要开发安全的软件……但我们知道的还不够。”这种呼声是本书的直接催化剂：向他们传授学校里不教的技术——如何设计、生成、测试和注释安全的软件。所谓“安全的软件”，并不是指安全代码或实现安全特性的代码，而是指为抵挡恶意攻击而设计的代码。安全的代码也是健壮的代码。

本书的目标是绝对要保证切实可行，书中可能使读者产生不安全感，可能会感到自己的代码也许会受到攻击。更确切地说，如果你创建的应用程序要运行在一台或多台计算机上，而这些计算机连到了网络上，或最大的网络Internet上，那么你的代码就可能会受到攻击。

系统安全受到威胁后会造成各种严重后果，如生产力下降、信誉受损以及财产损失，如果攻击者能够破坏应用程序的安全（如，使之无法使用），你的客户就可能会转而使用竞争对手的产品。在使用基于Internet的服务时，大多数人都没有耐心，如果你的服务不好用，客户也会投奔你的竞争对手。

对于众多软件开发商来说，真正的问题是，安全所带来的效益不像开发过程那样是显而易见的。因此，管理层不愿意在培训开发人员以编写安全的代码方面多花钱，在攻击得逞之前，他们不想在安全技术上投资。然而，亡羊补牢，则为时已晚。事后的修补工作，无论是在财力上还是在信誉上，都要付出高昂的代价。

历史证明，最好的方法是保护财产，使之免遭盗窃和攻击。我们的祖先早就制定了对盗窃、损坏或侵占他人财物者的惩罚措施。的确，人们都明白，私人财物应当受到保护。这些道德准则也适用于数字世界；因此，作为开发人员，我们的部分职责就是创建可保护数字资产的应用程序和解决方案。

本书包括一些基本概念，这些内容在学校课程里介绍“设计和构建安全的系统”主题时应当讲过。读者可能会认为，“设计”是设计人员或管理人员的事情，但作为开发人员和测试人员，同样也需要了解设计良好的系统结构以抵御攻击的有关过程。

众所周知，无论花多少时间和精力来开发软件，开发出的软件仍然会存在漏洞，因为人们无法预测未来的安全问题。对于Windows Server 2003来说，同样也存在一些漏洞；但按照本书

中所建议的方法，相信可以减少漏洞数，使黑客更难于发现和利用代码中的漏洞。

本书读者对象

本书适用于设计应用程序或生成、测试以及注释解决方案的人员。如果编写基于Web或基于Win32的应用程序，或者正在学习或开发基于Microsoft .NET框架的应用程序，本书同样是很好的读物。总之，只要工作中涉及到应用程序开发，都会在本书中找到许多值得学习的内容。

即使是正在编写不在Microsoft平台上运行的代码，书中的许多内容依然非常有用。除了个别几章是完全针对Microsoft平台以外，许多问题往往与平台无关。即便有时某种东西似乎仅适用于Windows，但其通常也有更加广泛的应用。例如，Everyone用户的“安全控制”访问控制列表和UNIX系统上设置为“全部可写”的文件，其实是同一问题，而跨网站的脚本问题是普遍存在的。

本书组织结构

本书分为五个部分。第一部分（第1～4章）概括说明了为什么要保护系统安全免遭攻击，以及设计这种系统的原则和分析技术。

第二部分和第三部分是本书的重点。第二部分（第5～14章）概括介绍了几乎适用于任何一种应用程序的重要的编码技术。第三部分（第15～18章）重点介绍了网络应用程序和.NET代码。

第四部分（第19～24章）讲述了一般图书中很少讨论的一些主题，如测试、进行安全代码审查、隐私策略以及安全的软件安装等问题。第23章介绍了放在其他各章都不太合适的一些一般原则。

第五部分是“附录”，包括5个附录，分别介绍危险的API，我们常听到的一些不考虑安全问题的荒谬借口，以及分别针对设计人员、开发人员和测试人员的安全措施核对清单。

与其他作者不同，我们不仅告诉你应用程序如何不安全，而且告诉你为什么人们不愿意构建安全的系统。本书绝对实用，书中解释了系统怎样会受到攻击，人们常犯的错误，以及如何构建安全的系统——这才是最重要的。

安装和使用范例文件

通过连接到站点http://www.microsoft.com/mspress/books/5957.asp，可以从Web上下载本书的范例文件（从Companion Content页下载）。要访问范例文件，请单击该页右侧More Information框中的Companion Content链接，打开Companion Content页，此页中包括下载范例文件的链接；也可以连接到Microsoft Press Support站点。下载链接可打开一个包含许可协议的可执行文件。要想把范例文件复制到硬盘上，请单击运行可执行文件的链接，然后接受许可协议。默认情况下，范例文件将被复制到My Document\Microsoft Press\Secureco2文件夹下。在安装过程中，可以改变目标文件夹。

系统要求

尽管可以使用包括Visual C++6.0在内的大多数编译器来编译本书中用C/C++编写的大多数范例，但还是要求读者安装Microsoft Visual Studio .NET。用Perl编写的范例已经使用ActiveState

Perl 5.6或ActivateState Visual Perl 1.0（可从http://www.activestate.com下载）测试过。VBScript和JScript代码已经用Windows Scripting Host测试过（Windows 2000及其以后的版本中包含Windows Scripting Host）。所有SQL范例都使用SQL Server 2000测试过。而Visual Basic .NET和Visual C#应用程序均是使用Visual Studio .NET编写和测试的。

本书中的所有应用程序（有两个例外），均可以在符合建议的系统要求的、运行Windows 2000的计算机上运行。第7章的Safer范例和第11章的UTF8 MultiByteToWideChar范例，必须在Windows XP或Windows Server 2003上才能正确运行。编译代码时必须使用更加健壮的机器（即比编译器所要求的基本条件更优）。

目　录

第二部分 安全的编码技术

第三部分 更安全的编码技术

第四部分 特殊的安全问题