Broadview
www.broadview.com.cn

Microsoft®

安全技术大系

Writing Secure Code for Windows Vista

在Windows Vista上编写安全的代码

【美】Michael Howard，David LeBlanc 著
罗爱国 郑艳杰 译

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

安全技术大系

在Windows Vista上编写安全的代码

【美】Michael Howard，David LeBlanc 著
罗爱国 郑艳杰 译

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

内 容 简 介

这份权威性的指南鼓励开发者为 Vista 平台编写更安全的代码，从而获得更多的客户。它为开发者提供了第一手的设计思路，对针对实际的安全问题给出具体的建议。本书介绍了 Vista 的一些新特性，包括 ACLs 和 BitLocker 等，此外它还丰富了一些以往的概念，例如防火墙和认证。

本书是《编写安全的代码》一书的最佳补充和扩展，是 Windows Vista 程序员的必备书目之一。

版权贸易合同登记号　图字：01-2007-4585

图书在版编目（CIP）数据

在 Windows Vista 上编写安全的代码 /（美）赫沃德（Howard,M.），（美）勒伯雷恩（LeBlanc,D.）著；罗爱国，郑艳杰译. —北京：电子工业出版社，2009.1
（安全技术大系）
书名原文：Writing Secure Code for Windows Vista
ISBN 978-7-121-07419-6

I. 在…　II. ①赫…　②勒…　③罗…　④ 郑…　III. 窗口软件，Windows Vista　IV. TP316.7

中国版本图书馆 CIP 数据核字（2008）第 146203 号

责任编辑：高洪霞
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：15　字数：79 千字
印　　次：2009 年 1 月第 1 次印刷
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，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

对于身处高技术产业的每一个人来说，《在 Windows Vista 上编写安全的代码》都是值得拥有的。书里表达的观念体现了创造可信赖用户体验里的最新思想。

Microsoft 认识到技术将随着摩尔定律应用到社会的各行各业，而更强大、更便宜的计算机将可以迎合所有人的需求。随着宽带网的持续普及，以及新的无线网络技术出现，全世界的计算机设备彼此相连，这给人们访问信息、媒体和服务带来了空前的便利。不单单是 Microsoft 有这种远见，它其实也是大部分高科技行业的共识。不论你是否迷信商业或技术，这个远见都给我们描绘了这样一幅图景：我们的行业将怎样高速增长，我们的商业将怎样大获成功，我们将怎样为全世界的人们提供越来越多的便利——每一个人都可以发掘他全部的潜能。这是一幅美妙的前景——我们已经迫不及待了。

为了实现这个前景，需要有一个基本的前提。如果各行各业的人都加入到我们这个美妙的、互连的数字世界，他们将需要一定的信任。他们想知道他们的隐私是否被适当地保护了。他们也想确定他们的关键信息不会被窃取或破坏。他们还想他们的体验更加可靠、简单。这一直都在艰难地发展。

在 Microsoft，我们跟踪黑客和与互联网相关的犯罪行动。现在的环境变得很复杂：从为了开玩笑和声望而黑入系统到有组织的犯罪。据不完全统计，全世界与互联网相关的犯罪导致了数十亿美元的损失。这些钱可以用来资助许多工程，这也意味着罪犯在寻找高科技产品里最晦涩的漏洞方面比以往更加执着了。“假设没有人会注意到产品里的漏洞”只是我们一厢情愿的想法。我们生活的时代如果有漏洞出现，就会有人注意并利用它。

当黑客为了获取更高的回报时，他们在共享漏洞信息方面也变得更有组织了。我们现在生活的环境是：罪犯擅长“武装”漏洞信息，使从发现这些漏洞到利用这些漏洞获利之间的时间间隔趋于 0。这些罪犯可以算是互联网上有组织犯罪的军火商，他们将这些商品

待价而沽。

因为恶意的黑客团伙比以往更有组织性，对于每一个生产高科技产品的人来说，使用严格的技术标准变得越来越重要了，例如《Secure Development Lifecycle》（已有中文版，名为《软件安全开发生命周期》），可以将产品里的漏洞降到最少。因为高科技产品也是人造的，所以并不能保证没有漏洞。然而，如果我们整个产业能联合起来，将可以使我们的防御最大化。

作为一个软件平台，Windows 在帮助软件公司交付更安全的软件方面，扮演着特殊的角色。《在 Windows Vista 上编写安全的代码》可以帮助那些为 Windows 编写应用程序的人遵循安全最佳实践，交付从根本上更安全的软件产品。Windows Vista 在设计时就考虑到了为软件作者提供相关的特性，从而使他们的软件更安全。这些特性体现了 Microsoft 对软件应用程序认证、数据保护、防范利用等方面的深刻理解。通过使用 Windows Vista 提供的安全特性，应用程序在客户眼里将会变得更安全，也更加可信。

实现数字化生活还有很长一段路要走，需要高技术行业协同工作，为人们提供便利和价值。成功的关键因素是创造出人们信任的技术产品。《在 Windows Vista 上编写安全的代码》将帮助我们向客户交付从根本上更安全更可信的产品。

Jon DeVaan
Senior Vice President of Engineering Excellence
Microsoft Corporation
February 2007

前　言

互联网上的计算机每天都可能会受到攻击和伤害。毫无疑问，攻击者正逐渐深入软件堆栈，攻击计算机上安装的软件。不过，这种情形正在慢慢变少，因为随着要求安全的呼声日益高涨，软件厂商在操作系统的防护方面投入了更多的人力物力。在 Windows XP 发布的 2001 年到 Windows Vista 发布的 2006 年期间，安全技术的发展可谓是日新月异，但反观另一方面，令人厌烦的低级攻击行为也在日益增多。我们经常听到有人抱怨 Windows 是最容易受到攻击的平台。的确如此，因此，下面的陈述可能会使他们更担心：我们（也就是本书的作者）对媒体上报道的攻击事件并不是特别在意，因为在我们看来攻击永远都会发生。其实，人们应该担心的是其产生的危害，正是因为这个原因，微软人从长计议，竭尽全力想把 Windows Vista 打造成更安全的产品。

Windows Vista 是微软公司发布的有史以来最安全的操作系统。我们向里面添加了很多防御性的设计（defensive engineering），也采用了很多防护措施。但令人遗憾的是，即使我们如此努力，但攻击仍将继续（我们可以尽量把自己的工作做得更好，但没有权利指定别人可以做什么，不可以做什么）。我们不是说 Windows Vista 没有安全 bug，它肯定会有，但我们为它增加了许多防护措施，尽量减小它被成功攻击的可能性，减少漏洞被利用的机会。我们加入这些防护措施的目的是尽量避免危害发生。

针对日益增长的潜在攻击威胁，你打算如何保护你的应用程序？记住，攻击迟早都会发生！仅仅因为应用程序的标题中没有“Microsoft”并不意味着不会被攻击，也并不意味着它永远不会被攻击！使安全成为一个令人着魔的主题的不是这样一些因素，比方说，计算机的性能和可靠性。性能与可靠性指的是人与计算机之间的问题，而安全却是人与人之间的较量。安全问题没有终结，因为这个世界上总有一些怀有恶意的人。

除了整理已有的代码、修正设计问题外，微软还为 Windows Vista 新增了许多功能，利用这些功能可以使应用程序更安全。不同于我们以前那些以介绍基础知识为主的书，本书

主要介绍运行在 Windows Vista 上的应用程序怎样利用系统提供的防护措施来保护用户。除了基本的防护策略外，本书还介绍了一些新的安全功能，你可以在应用程序中使用它们，以增加程序的防护措施，从而帮助你或你的客户达到商业目标。

Windows Vista 的安全之路走了 5 年多，在这 5 年多的时间里，微软向 Windows Vista 中增加了许多防护措施和新的安全功能。你可以在应用程序中充分利用它们，从而减少被攻击的机会。你可以选用下面介绍的三种方法：

- 减少用户——如果没有人用你的应用程序，你就不值得攻击。
- 减少攻击面——组件的入口越少（特别是默认情况下），被攻击的可能性也就越小。
- 加固攻击面——使攻击者知难而退。

我们不建议大家使用第一个方法，但如果你不重视安全，而且固执己见，基本上可以肯定会出现这种情形。我们希望后两个方法对你有所帮助，使你能利用操作系统提供的防护措施和功能保护用户，这也正是本书的目标——阐述如何在程序中使用 Windows Vista 提供的这些功能。

目标读者

这本书的目标读者主要是那些为 Windows Vista 编写软件的开发者。当然，这本书还包括一些软件设计上的内容，因此，软件设计师和系统架构师也会从中获益。不过要注意的是，书中包含了大量的代码。

我们将假设读者已经掌握 Windows 认证与授权等方面的基础知识。虽然书中提供了一些背景信息，但我们仍将假设你知道怎样在 Windows 里保护对象。如果你不知道，建议你先找一些像“*Windows Internals Fourth Edition*”（Mark Russinovich，David Solomon，Microsoft Press 2005）之类的书来读。

本书与“Writing Secure Code”（《编写安全的代码》）一书的关系

“Writing Secure Code”（微软出版社）第一版和第二版的内容主要是介绍关键的安全编

码的原则，除此之外，书中还简单介绍了在设计和测试软件时应该遵循的原则。而本书的主要内容是介绍怎么利用 Windows Vista 内部的防护措施和功能，编写出安全的代码。如果你已经有了《编写安全的代码》一书，本书也不会显得多余，因为本书的内容主要是面向 Windows Vista 的设计和编码的最佳实践，而《编写安全的代码》的内容是宽泛的、基础性的。因此，这本书不是“编写安全的代码”的超集，而是它的有益补充。

如何阅读本书

这本书很薄，如果你打算或正在 Windows Vista 下编写软件，那么，这本书就是为你准备的——因为你可以从中了解到微软在 Windows Vista 里新增或改进的防护措施和技术。

本书每一章的内容都相对独立，除了前三章——所有在 Windows Vista 下编写软件的开发者都应该阅读，其他章节可以有选择地阅读。

第 1 章，“代码质量”描述了我们为剔除潜在的安全 bug，在 Windows Vista 的代码层所做的改进。软件行业可以从微软为 Windows Vista 增加安全性所采取的措施中学到很多东西。

第 2 章“用户账号控制、令牌和完整性级别”和第 3 章“缓冲区溢出防护”是一定要读的，因为这两章介绍的技术影响着 Windows Vista 里所有其他的功能。

现在是网络时代，即使不是所有的开发者，至少大部分的开发者将会编写基于网络的应用程序，因此，应该熟读第 4 章“网络防护措施”，并学以致用。

编写服务程序的开发者应该仔细阅读第 5 章“创建安全而且能复原的服务”，因为我们提供的指导可以使得服务在面对攻击时更有弹性，并使创建以尽可能低的特权运行的服务变得更容易。

如果你为 IE 编写代码，比如说 BHO（browser helper objects）、工具条或 ActiveX 控件，那么你应该阅读第 6 章“利用 IE 的防护措施”。Windows Vista 的 IE 7 在架构上做了很多改进，并新增了许多防护措施，这些将影响代码的运行方式。

如果你的软件中使用了加密函数，那么你应该阅读第 7 章“加密方面的增强”，因为第 7 章除了介绍名为 Cryptography API：Next Generation（CNG）的新加密结构体系外，还增

加了更新的算法及证书的撤销与检验等内容。

开发企业级软件的程序员将从第 8 章“认证与授权”中找到需要的内容，本章简单地介绍了 Windows Vista 里的认证及 ACL 等概念。

最后一章“其他的防护措施和安全技术”介绍的是一些 Windows Vista 中新加的，但又不适合放在其他章节中的防护措施。你应该花一些时间阅读本章，从而确定在你的软件中是否采用这些功能和防护措施。

如何使用书中的代码

本书中的代码大部分是用 C/C++写的，只有很少一部分是用 C#写的，使用的开发环境是 Microsoft Visual Studio 2005 Team Suite Service Pack 1 和 Windows Software Development Kit（SDK）。对 C/C++开发来说，首先要安装 Visual Studio，接着安装 Windows SDK。除此之外，还要向 Visual Studio 中添加相关的 Windows SDK 头文件和库文件，从而使 Visual Studio 首先从更新后的目录读取。你可以按下面的步骤操作：

步骤 1 打开 Visual Studio；

步骤 2 选择工具|选项；

步骤 3 找到并展开项目和解决方案；

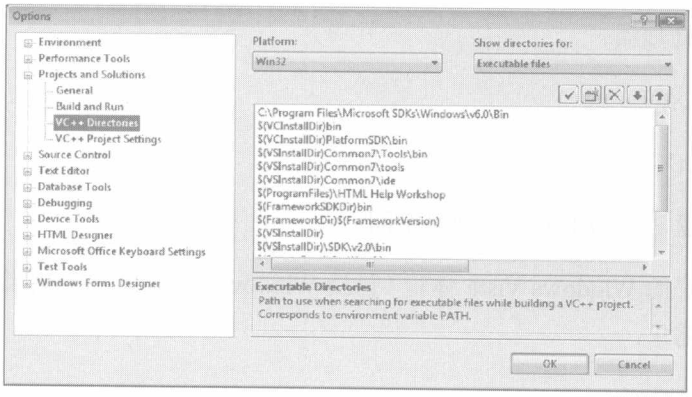
步骤 4 选择 VC++目录；

步骤 5 单击新行图标；

步骤 6 增加 Windows SDK include files 所在的目录路径。

重复上面的步骤添加可执行文件和库文件。下图显示的对话框可以说明正在讨论的问题。当然，你也可以在安装 SDK 时接受更新环境变量的选项——记得要重启开发环境。

最后，在你的应用程序中，你应当在包含其他头文件之前增加下面这一行，插入在 stdafx.h 文件的第一行比较合适。




```
#define _WIN32_WINNT 0x0600
```

如果你的代码中没有这一语句，而又引用了 Windows Vista 中新增的函数、定义、常量或结构时，可能无法通过编译。

重要 注意，书中所有的 C/C++例子代码在合适的地方都用了 SAL（在第 1 章里介绍），用 warning level 4（/W4）编译时不会出现警告，也没有 PREfast 警告（/analyze），当然，我们用于演示不安全的编程实践的例子除外。

对于 C#开发来说，只要程序是在安装了 Windows Vista 计算机上运行，就不需要更改开发环境的任何设置。

本书配套的网站上有什么?

本书讨论的所有的代码例子都可以从配套的 Web 页面上下载，地址是：

http://www.microsoft.com/mspress/companion/0978735623934

请你务必先读一下 readme 文件，该文件中对所有的例子代码做了介绍。

系统需求

任何能运行 Windows Vista 的机器都能运行本书里的例子代码（可以在配套的 Web 网站上下载），运行 Windows Vista 的最低需求是：

- 800 MHz 处理器
- 512 MB 内存
- 支持 DirectX 9 的显卡
- 20 GB 硬盘，15 GB 可用的硬盘空间

为了获得更好的 Windows Vista 体验（包括 Windows Aero 的视觉效果），你的计算机至少需要满足以下需求：

- 1GHz 处理器
- 1 GB 内存
- 支持 DirecteX 9 的显卡，支持 Windows Vista Display Driver Model（WDDM）的显示器，128 MB 显存（如果 GPU 使用共享内存，则不需要独立显存），Pixel Shader 2.0，每像素 32 位。
- 40GB 硬盘，15 GB 可用的硬盘空间
- 内/外置 DVD-ROM
- 声卡
- 可以访问互联网

目　录