HZ BOOKS
华章科技

全面、系统、深刻揭示.NET平台的安全机制和工作原理，为构建安全的.NET应用以及ASP.NET、WCF、WPF、Silverlight、Open XML和WIF等应用提供绝佳实践指导

實戰

杨文海 鲁凤芝 何平 等著

Uncover .NET Security: Building Safety .NET Applications

.NET安全揭秘

机械工业出版社
China Machine Press

實戰

Uncover .NET Security: Building Safety .NET Applications

.NET安全揭秘

杨文海 鲁凤芝 何 平 贺立华
杨博宇 武 伟 郝志刚 甄建廷 著

机械工业出版社
China Machine Press

作为 .NET 程序员、.NET 应用架构师和 .NET 安全工作人员，如何才能开发和设计出安全的 .NET 应用？如何才能维护和保证 .NET 应用系统的安全性？本书是资深 .NET 专家和安全专家多年工作经验的结晶，深刻揭示了 .NET 系统（涵盖 .NET 平台本身、ASP.NET、WCF、Silverlight、Windows Azure、Open XML 和 WIF 等）的安全特性及其工作原理，系统而全面地讲解了构建安全的 .NET 应用所必须掌握的所有理论知识，并包含大量最佳实践。

全书共分为五个部分。第一部分：.NET 安全基础，透彻讲解了 .NET 体系结构、程序集与反射、应用程序域和 CLR 寄宿等核心技术，这部分内容是 .NET 架构的核心，同时也是理解 .NET 底层安全机制的基础；第二部分：.NET 平台安全性，深入分析了代码访问的安全性和基于角色的安全性的原理，这部分内容既是 .NET 应用框架安全性的基础，也是整个 .NET 平台体系安全性的核心；第三部分：数据安全，深刻阐述了数据加密、数据存储和数据通信的安全性，这部分内容介于 .NET 平台底层安全性与 .NET 应用安全性之间，是联系二者的纽带；第四部分：.NET 应用安全性，全面讲解 .NET 平台下 ASP.NET、WCF、WPF、Silverlight 和 Open XML 等常用框架和技术的安全机制与原理；第五部分：高级扩展，重点介绍了最新的 WIF 框架和 Windows Azure 的安全性，这是 .NET 安全领域未来的重心之一。

本书是构建安全 .NET 应用的百科全书，适合所有关注和学习 .NET 安全的读者阅读。

图书在版编目（CIP）数据

. NET 安全揭秘 / 杨文海等著 . —北京：机械工业出版社，2012.4

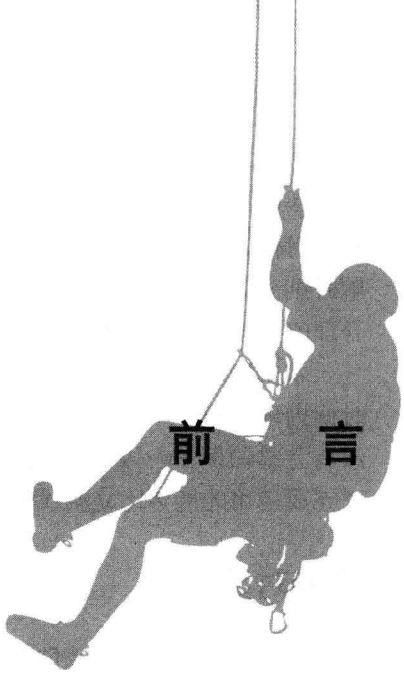
ISBN 978-7-111-37573-9

I. N…　II. 杨…　III. 计算机网络 – 安全技术　IV. TP393.08

中国版本图书馆 CIP 数据核字（2012）第 032480 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：朱秀英
北京京师印务有限公司印刷
2012 年 5 月第 1 版第 1 次印刷
186mm×240mm • 42 印张
标准书号：ISBN 978-7-111-37573-9
定价：89.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com



前　言

为什么要写这本书

我从小就喜欢读武侠小说，想成为绝世高手，风度翩翩，武功高强，行侠仗义。大学读了计算机专业，我又认为黑客就是计算机世界里的大侠。工作之后，我与 C# 一见钟情，她的优雅和简洁令我着迷。从认识她的那一刻开始，我抛弃了 C++ 和 Java，发誓只爱她一个。爱屋及乌，我成了 .NET 的忠实信徒，虔诚而狂热。也正是因为对 .NET 的狂热，我希望她更安全。

当安全问题日益严重时，.NET 没有令我失望，依然优秀。当我再次投身安全领域，我的世界不再只有 .NET，这也使我换了一个角度来审视她，来研究她的安全。

对于专注业务的程序员来说，重新构建一个安全的系统成本太高。即使是一个安全专家，也面临着将许多的安全方案用代码来实现的困境。虽然不能实现不用敲一行代码就解决这些问题，但是作为 .NET 开发人员，可以将问题变得更简单。因为 .NET 在设计之初就考虑了安全性问题，而且在迈向面向服务的进程中，还诞生了专注于安全的框架。

但是可惜的是，大部分开发人员竟然对 .NET 安全性一无所知。因此，我想将自己在实践中总结出来的经验和体会与大家分享，希望每一个 .NET 开发人员都能从中受益，让应用更安全、更健壮，让自我开发的安全框架更简洁，让开发过程更轻松。

本书特点

在创作本书的过程中，我也在不断地思考安全原理和安全应用的取舍问题，思虑再三，最后决定按照自己的实践经验和想法来决定重点知识的结构安排。

本书立足 .NET 平台，但是所讲的内容并不只针对 .NET 开发人员。我更想通过这本书，

将这些安全基础理论和安全架构的方式传达给更多的读者。在对一些通用的安全基础进行讲解的时候，我更倾向于将重点放在理论上而不是 .NET 平台的实现上，在对其他内容进行讲解时则又将侧重点放在 .NET 本身，这样的结构安排是经过仔细斟酌的。当然，如果你有更合理的方案可以提出来，很高兴与你一起探讨。

本书包含了 .NET 安全性的所有核心主题。在写这本书的时候，力求使读者能在最短的时间内理解每一个概念，了解基本的框架、流程、原理和使用方法。在具体的应用上，本书没有完整的例子，因为本书想传达的是理念。我坚持认为，通过学习本书内容之后，掌握独立完成应用的能力比复制代码更重要。

读者对象

这不是一本讲黑客攻防的书，如果想从这本书中得到关于黑客攻击的技术细节，那么你会很失望；如果你想从这本书中得到如何防守跨站攻击、SQL 注入或者网页木马的实施细节，你也将会失望。这是一本面向开发人员和安全专家的书，重点讲解 .NET 平台体现出来的基本安全理论，对于专注于安全的任何群体来说，这都是必须掌握的。

本书的读者对象包括：

- 有一定开发经验的 .NET 程序员
- 专注于 .NET 安全的安全技术工程师
- .NET 应用架构师
- 高校计算机相关专业和 .NET 培训机构的老师和学生
- 互联网架构师
- 对计算机和网络安全感兴趣的爱好者

本书的内容

本书共分为五个部分，五个部分之间既相互独立又相辅相成。

第一部分（第 1 章～第 3 章）讲解了 .NET 安全的基础，这是 .NET 架构的核心部分。具体内容包括 .NET 体系结构、程序集和反射、应用程序域和 CLR 寄宿的原理。第一部分提到的核心概念是全书所有章节都会反复提到的。如果还没有对 .NET 的底层原理了解得很透彻，建议认真阅读这一部分。

第二部分（第 4 章～第 5 章）讲解了 .NET 的平台级安全性。这些内容是整个 .NET 应用框架安全性的基础，没有这些基础是无法继续阅读的。这是本书的必读部分。在这一部分我们将具体了解到代码访问安全的原理和基于角色的安全性，这是整个 .NET 安全性的核心概念。后文的应用安全环节与之重复的部分大都省略了细节，所以建议务必仔细阅读此部分。

第三部分（第 6 章～第 8 章）是数据安全部分。这一部分直接建立在第二部分的基础之上，介于底层安全性和应用安全之间。在这一部分中，我们会分析很多通用安全概念的原理，其中包括加密、解密、数字证书和签名，以及数据存储安全和通信安全。这部分的内容是许多安全应用和安全协议的基础，有助于了解很多基础概念的原理和常用加密算法的数学解释。

第四部分（第 9 章～第 14 章）是应用安全部分。主要内容集中在 .NET 平台的几种常用应用框架的安全上，是 .NET 开发人员的必读部分。这一部分根据实际情况对部分应用的安全原理作了详细解析，并针对部分应用给出了详细的示例，以确保读者能从原理和实践上完全掌握这部分内容。

第五部分（第 15 章～第 16 章）是高级扩展部分。这一部分介绍了最新的 WIF 框架和云安全的内容，这是 .NET 安全的未来趋势。

勘误和支持

参加本书编写的还有我的老师鲁凤芝女士，北森公司的同事何平、贺立华、杨博宇、武伟、郝志刚、甄建廷。由于作者水平有限，编写时间仓促，书中难免会出现一些错误或疏漏，恳请读者批评指正。欢迎访问我的博客（http://www.cnblogs.com/xuanhun）或发邮件（xuanhun521@126.com）与我交流。不论是批评还是褒扬，您的反馈都是对本书的关爱。

致谢

在本书的写作过程中，我得到了很多朋友、老师、同事及家人的大力帮助。

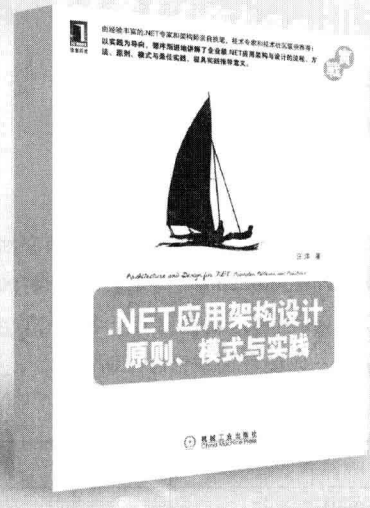
感谢机械工业出版社华章公司的编辑杨福川和白宇，没有你们的耐心、宽容和鼓励，恐怕我连完成这本书的勇气都没有。

最后要感谢我的父母、老师及所有培养我的人。当然，还要感谢我的女朋友小白。

谨以此书，献给我最亲爱的家人，以及众多关注 .NET 和计算机安全的人们！

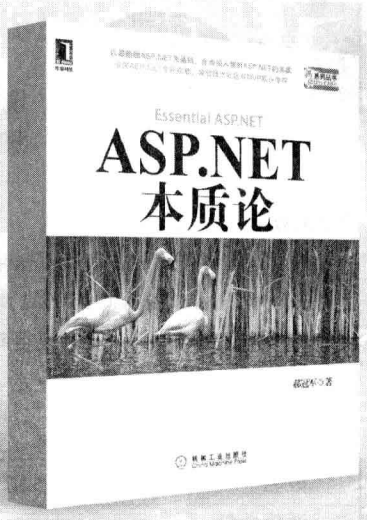
杨文海

2012 年 3 月于北京



.NET领域畅销书，由经验丰富的.NET专家和架构师亲自执笔，技术专家和技术社区联袂推荐！

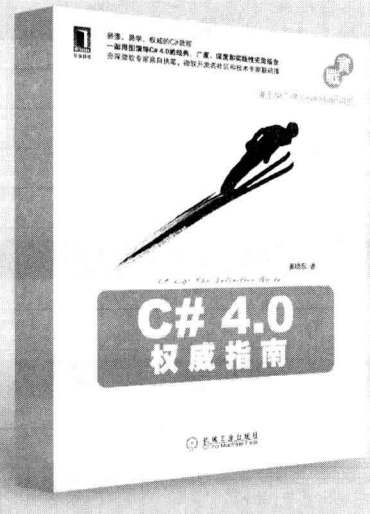
以实践为导向，循序渐进地讲解了企业级.NET应用的架构与设计的流程、方法、原则、模式与最佳实践，极具实践指导意义。



ASP.NET领域畅销书，繁体版在中国台湾同步发行

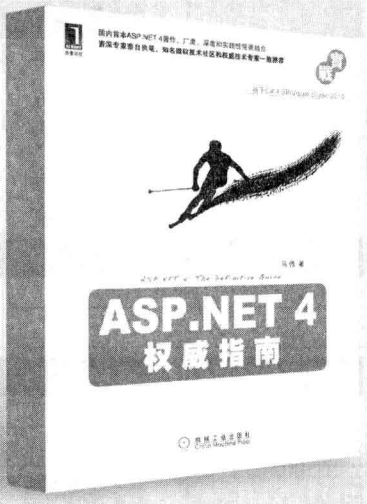
深入剖析ASP.NET的运行机制和工作原理，带你领略ASP.NET的本质和精髓

包含大量开发技巧和最佳实践，为开发稳定而高效的ASP.NET应用提供绝佳指导



C#领域畅销书，繁体版在中国台湾同步发行

资深专家亲自执笔，知名微软技术社区和权威技术专家一致推荐，用图演绎C# 4.0的经典，广度、深度和实践性完美结合



ASP.NET领域畅销书，繁体版在中国台湾同步发行

资深专家亲自执笔，知名微软技术社区和权威技术专家一致推荐，广度、深度和实践性完美结合，公认的权威著作

www.hzbook.com

填写读者调查表　加入华章书友会
获赠精彩技术书　参与活动和抽奖

尊敬的读者：

感谢您选择华章图书。为了聆听您的意见，以便我们能够为您提供更优秀的图书产品，敬请您抽出宝贵的时间填写本表，并按底部的地址邮寄给我们（您也可通过www.hzbook.com填写本表）。您将加入我们的"华章书友会"，及时获得新书资讯，免费参加书友会活动。我们将定期选出若干名热心读者，免费赠送我们出版的图书。请一定填写书名书号并留全您的联系信息，以便我们联络您，谢谢！

书名：　　书号：7-111-(　　)

姓名：	性别：☐男　☐女	年龄：	职业：
通信地址：		E-mail：	
电话：	手机：	邮编：	

1. 您是如何获知本书的：

☐朋友推荐　☐书店　☐图书目录　☐杂志、报纸、网络等　☐其他

2. 您从哪里购买本书：

☐新华书店　☐计算机专业书店　☐网上书店　☐其他

3. 您对本书的评价是：

技术内容	☐很好	☐一般	☐较差	☐理由_____
文字质量	☐很好	☐一般	☐较差	☐理由_____
版式封面	☐很好	☐一般	☐较差	☐理由_____
印装质量	☐很好	☐一般	☐较差	☐理由_____
图书定价	☐太高	☐合适	☐较低	☐理由_____

4. 您希望我们的图书在哪些方面进行改进？

_____

_____

5. 您最希望我们出版哪方面的图书？如果有英文版请写出书名。

_____

_____

6. 您有没有写作或翻译技术图书的想法？

☐是，我的计划是_____　☐否

7. 您希望获取图书信息的形式：

☐邮件　☐信函　☐短信　☐其他_____

请寄：北京市西城区百万庄南街1号　机械工业出版社　华章公司　计算机图书策划部收

邮编：100037　电话：（010）88379512　传真：（010）68311602　E-mail: hzjsj@hzbook.com

目 录

第三部分　数据安全