Programming .NET Security

.NET安全编程 (C#/VB.NET)

Adam Freeman & Allen Jones 著
靳京 译

O'REILLY®
清华大学出版社

.NET 安全编程

(C#/VB.NET)

Adam Freeman & Allen Jones 著

靳京 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权清华大学出版社出版

清华大学出版社

北京市版权局著作权合同登记
图字：01-2006-7112 号

图书在版编目（CIP）数据

.NET 安全编程（C#/VB.NET）/（美）弗里曼（Freeman, A.），（美）琼斯（Jones, A.）著；靳京译. —北京：清华大学出版社，2007.2
书名原文：Programming .NET Security
ISBN 978-7-302-14500-4

I. N… II. ①弗… ②琼… ③靳… III. 计算机网络－程序设计 IV. TP393

中国版本图书馆 CIP 数据核字（2007）第 003796 号

责任编辑：常晓波
封面设计：Ellie Volckhausen，张健
责任校对：张　剑
责任印制：王秀菊

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
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：178 毫米×233 毫米　43 印张　　**字　　数**：924 千字
版　　次：2007 年 2 月第 1 版　　**印　　次**：2007 年 2 月第 1 次印刷
印　　数：1～3000 册
定　　价：79.00 元(册)

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：023384-01

O'Reilly Media, Inc. 介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc. 授权清华大学出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 Unix、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的 *The Whole Internet User's Guide & Catalog*（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc. 一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc. 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得 O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以O'Reilly Media, Inc. 知道市场上真正需要什么图书。

目录

第 4 部分 .NET 应用程序框架

第 5 部分 API 快速参考

前言

.NET Framework 是为满足商业组织和个人需求、为支持多种应用程序模型而开发的一种灵活的通用计算平台。.NET汇集了业界发展的最新趋势，它支持高度分布式系统、基于组件的应用程序和基于 Web 的服务器解决方案（包括 XML Web 服务）。这些新趋势改进了应用程序的功能，提高了程序员的效率，但是它们也要求软件用户、软件制造商和服务提供商密切关注软件和系统的安全。

从传统角度来看，程序员都把安全看做是“马后炮”；然而，现在越来越多人认为安全是一种需求而不是一种选择，因为现在的应用程序都需要把安全集成到它们的开发过程中。这是一个简单的事实，即在开发.NET应用程序时不能忽视安全，因为安全位于.NET Framework 的核心并隐含于编写的应用程序中。即使仅为了响应 .NET Framework 的默认操作，也必须理解如何对 .NET 安全性进行编程；更重要的是，这样做是为了编写深受欢迎的有效且实用的 .NET 应用程序。

本书组织结构

本书分为 5 部分。第 I 部分介绍了软件安全的基本概念。第 II 部分讨论了如何编写 .NET 运行库的安全功能。第 III 部分阐述了如何以编程方式使用 .NET 类库中的密码类。第 IV 部分讨论了如何使用与程序运行平台有关的安全功能。最后，第 V 部分介绍了本书中的安全类涉及的所有 API 参考。

第 I 部分：基础

第 1 章 安全基础

本章介绍了软件安全的一些基本概念，在阅读后续章节之前应该理解这些概念。本

章说明了安全的必要性和软件安全的目的。本章还介绍了在开发自己的安全编程技术时应注意的一些重要环节。

第2章 程序集

本章概述了.NET程序集，它是.NET安全的一个关键组件。本章阐述了程序集的结构和内容，示范如何创建不同类型的程序集，以及讨论如何保护程序集不被篡改和逆向工程。

第3章 应用程序域

本章介绍了应用程序域的作用，讨论了应用程序域对应用程序隔离、安全和配置的影响。

第4章 安全应用程序的生命周期

本章介绍了软件安全性以何种方式集成进应用程序的生命周期中，并且提供了实际的建议以帮助读者理解后续章节所涉及的内容。

第II部分：.NET安全性

第5章 运行库安全性介绍

本章介绍了.NET运行库提供的主要安全功能；解释了它们的目的和作用，它们如何交互，以及它们与底层操作系统提供的安全之间有何关系。

第6章 证据和代码标识

本章介绍了什么是证据，证据从何而来，使用证据的目的及如何使用不同类型证据（包括.NET Framework提供的标准证据类集合）。本章还示范了如何在编程中使用证据，如何在开发用户证据类时扩展.NET Framework的安全功能。

第7章 权限

本章介绍了什么是权限及其在实现代码访问安全性时的作用。本章还描述了运行库使用何种机制实现代码访问安全性，如何使用权限操作这些机制。最后，本章为读者介绍了在实现自己的用户权限时如何扩展代码访问安全性。

第8章 安全策略

本章介绍了.NET运行库如何使用安全策略来决定授予一个程序集或应用程序域哪类权限，安全策略的结构及运行库的组件如何交互。本章还说明了如何在编程时使用安全策略，并示范如何使用应用程序域策略。

第9章 管理代码访问安全性

本章概述了.NET Framework运行的默认安全策略，讨论了如何使用.NET的安全工具来管理安全策略。

第 10 章 基于角色的安全性

本章讨论了什么是基于角色的安全和执行.NET Framework。本章还阐述了用于访问基于角色安全的类，示范如何在程序中使用这些类。

第 11 章 隔离存储器

本章介绍了什么是隔离存储器，说明了隔离存储器会给数据存储选项带来何种优势。本章还示范了如何在编程中使用隔离存储器，以及如何管理和控制对隔离存储器的访问。

第 III 部分：.NET 加密

第 12 章 介绍加密

本章概述了加密的不同方面，讨论了加密应该注意的一些危险和限制。

第 13 章 散列算法

本章深入探讨了散列码，如何使用.NET Framework 类库创建和运行散列码，以及如何通过增加新的散列算法来扩展 .NET Framework。

第 14 章 对称加密

本章讨论了如何使用对称数据加密实现机密性，如何使用.NET Framework加密和解密数据。本章还阐述了如何通过增加新的对称加密算法来扩展.NET Framework。

第 15 章 非对称加密

本章介绍了什么是非对称加密及其工作机制，阐述了非对称加密如何解决密钥交换的问题，示范了如何通过增加新的非对称加密算法来扩展 .NET Framework。

第 16 章 数字签名

本章介绍了什么是数字签名及其工作机制，如何在.NET应用程序中使用数字签名。本章还示范了如何通过增加支持用户数字签名算法来扩展 .NET Framework。

第 17 章 加密密钥

本章讨论了.NET Framework以何种方式支持密钥、密钥的重要性和如何创建密钥。

第 IV 部分：.NET 应用程序框架

第 18 章 ASP.NET 应用程序安全性

本章描述了使用何种功能增加ASP.NET应用程序的安全性，讨论了ASP.NET应用程序安全性的所有问题，.NET Framework 执行何种机制来提供验证、授权和为 ASP.NET 应用程序提供服务。

第 19 章 COM+ 安全

本章讨论了 COM+ 安全服务和如何在 COM+ 组件里运用安全服务。

第20章 事件日志服务

本章讨论了如何从 .NET 应用程序中使用 Windows 事件日志服务以检查 Windows 安全事件。

第 V 部分：API 快速参考

第 V 部分全面地介绍了 API 参考，它们涉及到的 .NET Framework 基础类库中与安全有关的命名空间如下所示：

```
System.Security
System.Security.Cryptography
System.Security.Cryptography.X509Certificates
System.Security.Cryptography.Xml
System.Security.Permissions
System.Security.Policy
System.Security.Principal
```

本书读者对象

本书为两组人群而编写。第一组是 .NET 应用程序的架构师和设计人员，他们必须懂得 .NET 安全的作用和局限性以便将其运用到设计和计划中。第 II、III 和 IV 部分的每一章开始都详细讨论了这些技术，但是并没有详述各个类和方法。

第二组是 C# 和 Visual Basic .NET 的程序员，他们想知道如何使用 .NET Framework 的功能来编写更多的安全应用程序。在第 II、III 和 IV 部分每一章技术介绍之后，本书都详细阐述了如何编程运用 .NET Framework 的功能，并列举了大量的代码实例来解释书中的观点。

本书建议

本书主要是针对 .NET Framework 的安全编程；我们没有要求读者有先前对 .NET 安全类库的接触，但是仍希望读者是具有基本经验的 C# 或 Visual Basic .NET 程序员。

本书第 V 部分讨论了 .NET 应用程序的安全功能、Windows 平台的安全功能和其他外部服务之间的交互。在阅读这些章节时希望读者已熟悉外部技术，只需把注意力集中在安全编程方面。

本书约定

本书使用的字形惯例如下所示：

斜体字（*Italic*）：

- 路径名、文件名和程序名
- Internet 地址，例如域名和 URL
- 本书定义的新名词

等宽字体（`Constant Width`）：

- 命令行，需要逐字输入的选项
- 程序例子里的名字和关键字（包括方法名、变量名和类名）

等宽黑体（**`Constant Width Bold`**）

- 编程代码里强调的部分

与我们联系

我们已尽最大努力修正了本书，但如果读者发现任何错误，请写信告诉我们：

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

100080 北京市海淀区知春路 49 号希格玛公寓 B 座 809 室
奥莱理软件（北京）有限公司

本书的网页上列出了勘误表、示例和任何额外的信息。可登录以下网址查询：

http://www.oreilly.com/catalog/prognetsec

http://www.oreilly.com.cn/book.php?bn=978-7-302-14500-4

如果想要发表关于本书的评论和技术问题，请发邮件至：

bookquestions@oreilly.com
info@mail.oreilly.com.cn

关于图书、会议、资源中心和O'Reilly网络的更多信息，请查看我们的站点：

http://www.oreilly.com
http://www.oreilly.com.cn

参加本书翻译的人员有：靳京、陈宗斌、蔡京平、李毅、毕蓉蓉、祁海生、张贺乾、史宁、刘绿生、孙雷、蔡加双、安东辉、米翔娟、刘颜、王宇宇、沈程亮、陆晓萍、金国良、俞群、李正智、赵敏、陈征、陈红霞、张景友、易小丽、陈婷、管学岗、王新彦、金惠敏、张海峰、徐晔、戴锋、张德福、张士华、张锁玲、杜明宗、高玉琢、王涛、刘晓捷、董礼、何永利、李楠、陈宁、房金萍、黄骏衡、黄绪民、焦敬俭、李军、刘瑞东、潘曙光、蒲书箴、邵长凯、郁琪琳、张广东、梁永翔、刘冀得、孙先国、张淑芝、张路红、程明、李大成、张春林、刘淑妮、侯经国、宫飞、高德杰、李振国、孙玲、申川。

第 1 部分

基础

第 I 部分讨论了安全的必要性，介绍了开发安全软件所用的方法。该部分所含章节还介绍了程序集和应用程序域——.NET 应用程序的两个基本构件，它们对开发安全的软件至关重要：

第 1 章 安全基础

第 2 章 程序集

第 3 章 应用程序域

第 4 章 安全应用程序的生命周期