HZ BOOKS

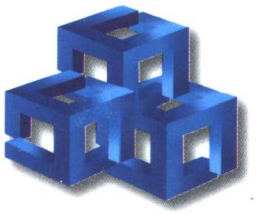
Designed for Microsoft® Windows NT® Windows® 98

附 赠 CD-ROM

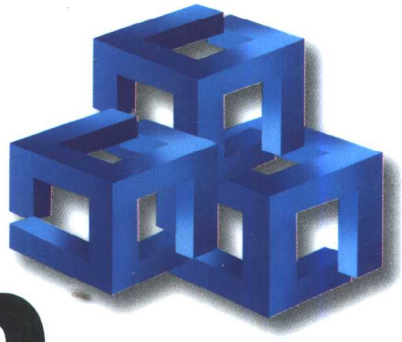
Designing Secure Web-Based Applications for Microsoft Windows 2000

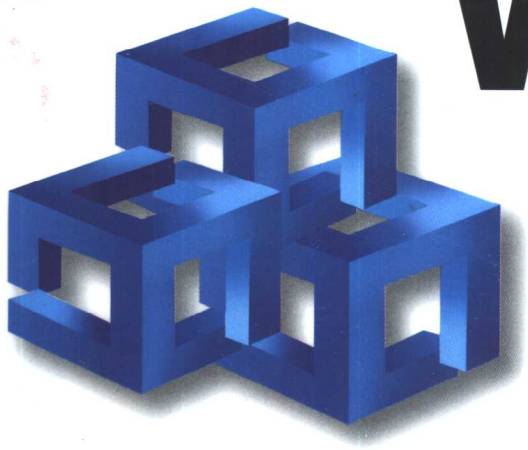
微软公司核心技术书库

(美) Michael Howard Marc Levy Richard Waymire 著
王建华 等译



Windows 2000 安全 Web 应用程序设计





机械工业出版社
China Machine Press

Microsoft Press

微软公司核心技术书库

Windows 2000 安全 Web应用程序设计

Michael Howard
(美) Marc Levy 著
Richard Waymire
王建华 等译

机械工业出版社
China Machine Press

本书对Windows 2000的所有主要安全服务程序进行了权威性的介绍，并且讨论了Windows 2000、Microsoft Internet Explorer、Internet Information Services、Microsoft SQL Server和COM+的安全特性，展示了各个“独立的”安全问题互相之间的关系，以及如何将相应的安全特性应用于网络环境和应用程序，以便降低网络的安全风险。还介绍了一些非常重要的安全问题，比如对安全风险的分析，对网格构成的各种威胁，身份验证，访问权的授权检查，个人信息的保密等。本书所附的光盘包括书中示例程序代码、参考信息等。

本书版权登记号：图字：01-2000-3124

图书在版编目（CIP）数据

Windows 2000安全Web应用程序设计 /(美) 何沃德(Howard, M.)等著；王建华等译. - 北京：机械工业出版社，2001.3

(微软公司核心技术书库)

书名原文：Designing Secure Web-Based Applications for Microsoft Windows 2000

ISBN 7-111-08770-4

Ⅰ.W… Ⅱ.①何… ②王… Ⅲ.①因特网-安全技术 ②因特网-站点-设计， Ⅳ.TP393.4

中国版本图书馆CIP数据核字(2001)第13547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：张鸿斌 薛怀云

北京市密云县印刷厂印刷·新华书店北京发行所发行

2001年4月第1版第1次印刷

787mm×1092mm 1/16·23.75印张

印数：0 001-5 000册

定价：55.00元(附光盘)

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

译 者 序

近年来，随着Internet应用得到迅速而广泛的普及，计算机网络的安全问题越来越成为人们关注的焦点。人们还记得，1999年下半年，有人对Internet实施了分布式拒绝服务的攻击，使网络充塞着大量的恶意信息，结果导致美国的几家最大的网络公司运营陷入瘫痪，长时间无法为用户提供服务。黑客的攻击也令人们担心电子商务的安全，人们害怕金融交易和个人认证信息被他人窃取。关于黑客攻击网络窃取机密信息的报道也经常见诸于报端。他们有的利用协议运行中出现的漏洞，有的利用TCP/IP本身设计中存在的缺陷，对网络频频实施攻击，使网络难以正常运行。

网络遭受的攻击次数正在不断增加，而且这些攻击带来的危害性也在逐步升级。从1999年8月到10月，Windows 2000安全小组对Internet上托管的一个运行Windows 2000的服务器进行了安全性测试，结果发现在此短短的3个月中，该服务器总共受到了60万次攻击。为此，人们迫切希望Internet应用程序和操作系统的安全性不断加以提高，一些基本组件，比如客户机和服务器上的操作系统、Internet浏览器、Web服务器、通信中间软件以及数据库和协同运行的服务器等，都具备更加安全的功能。

Microsoft Windows 2000以及相关的配套软件的推出，大大减轻了应用程序开发人员在设计安全特性时面临的负担，并且有助于他们更好地进行网络的安全管理。本书为网络管理人员和应用程序开发人员提供了应用程序开发过程中需要的各种安全信息。它不仅提供了必要的安全理论知识，而且重点对Internet Explorer、IIS、COM+和SQL Server的安全特性进行了介绍，同时详细说明了安全特性的最佳配置方法。Web开发人员将可以学习如何预先将各种安全特性纳入他们的应用程序，还可以了解如何解决和处理好系统的性能、速度与安全性之间的平衡问题。Web管理员能够了解如何安全地配置Web应用程序，如何确定计算机是否处于黑客的攻击之下，如何对黑客的攻击作出反应。

本书分四个部分共15章。第一部分“安全性概述与安全应用程序的设计”对网络安全的原则、各种网络安全问题以及对网络安全构成的威胁的种类进行了概要的描述，并且根据一个实例来说明如何进行安全应用程序的设计。第二部分“各种不同的安全技术及其利弊的权衡”介绍了Windows 2000、Microsoft Internet Explorer 5、Internet Information Services 5、SQL Server 2000和COM+ 1.0的安全特性和功能。然后讲述选择不同类型的安全技术时如何进行利弊的权衡，以满足网络安全原则的要求。第三部分“实际应用”介绍如何使用各种安全技术和策略为规定的情景建立安全应用程序，如何对应用程序的结构进行故障诊断，以及将应用程序放到Web上去运行时将会产生什么样的效果。第四部分“参考信息”介绍如何使用Windows 2000中的工具和脚本编程界面来建立定制的、可远程控制的管理脚本，并且讲述了Windows 2000中的Kerberos身份验证和加密及证书应用技术。

本书还配有一张光盘，它包含了一些示例代码和工具，可以用来开发基于Web的安全应用程

序。光盘中还包含了本书的电子版，它配有本书所没有的6个附录。提供了许多非常有价值的信息。

本书由王建华、杨宝明、蒋小英、王卫峰、侯丽坤、陈晓明等翻译，张晓佳录入，王建华校对。由于译者水平所限，译文中的不妥之处在所难免，敬请读者批评指正。

2000年11月

序　言

近年来，Internet应用得到了迅速的发展。最初的应用只是一些简单的信息发布Web站点，主要提供静态HTML内容（配有少量的服务器端脚本，用于满足各种不同的Web浏览器的需要），并且能够提供简单的站点个性化特性，也可以供搜索引擎用作查询处理器。今天，多层次分布式应用程序使用Microsoft Internet Explorer或者Netscape Navigator的脚本编程功能，能够建立基于Web服务器的“中间层”服务程序。这些应用程序常常是用CGI、ASP或者ISAPI编写而成的，用于访问数据库或者信息服务器。这些应用程序可以取代企业内部网中传统的客户机/服务器的应用程序，形成了新型的企业对企业的应用程序，从而开始改变企业的原材料供应渠道系统，并且提供与经营合作伙伴展开协作的更高效率的手段。

作为Microsoft公司的Windows NT系统安全业务部主任，我发现目前对这些Web应用程序的安全的攻击次数不断增加，而且攻击的严重性逐步升级。公众对安全问题的关注原先主要集中在对个人隐私信息的保护上（因为它关系到对金融交易和个人认证信息的保护），加之能够破坏数据完整性的计算机病毒迅速扩散，因此要求Internet应用程序和操作系统的安全性必须不断加以提高。我认为，如果要提高这些应用程序的总体安全性，有3项重要的工作必须完成。首先，系统管理员和数据中心的操作人员必须增强对安全威胁的意识，并且采取相应的最佳措施，防止计算机系统遭受这些威胁。第二，应用程序开发人员必须预先将安全特性设置在代码之中，而不是在发现安全问题之后才采取补救措施。最后，一些基本组件，包括基本的操作系统（客户机和服务器上的操作系统）、Internet浏览器、Web服务器、通信中间软件以及数据库和协同操作服务器等，都必须具备必要的安全功能，这样就不需要由应用程序来实现这些安全功能。与安全性相关的讨论涉及的问题很多，说明最终用户、软件开发人员和IT专业人员越来越重视和提高他们系统的总体安全性。他们面临的问题是，大量的著作、白皮书和Web站点上的信息目不暇接，因此大多数人难以找到他们需要的便于理解的信息。许多大专院校的计算机科学课程中关于安全问题的教学内容主要集中在安全理论问题上，这只能解决部分的系统安全问题。而业界咨询机构又没有能力满足人们的需求。

随着Microsoft Windows 2000的问世，以及相应的Internet Explorer、Internet Information Services（IIS）、Exchange和SQL Server的推出和应用推广，我相信Microsoft公司在减轻应用程序开发人员在设计安全特性时面临的负担和帮助他们从事安全性管理等问题上已经取得了重大的进展。本书为管理人员和应用程序开发人员提供了应用程序开发过程中需要的各种安全信息。由于本书不仅提供了“必要的”安全理论知识，而且对Internet Explorer、IIS、COM+和SQL Server的安全特性的功能进行了重点的介绍，同时按步骤对安全特性的最佳配置方法进行了系统的说明，因此你可以全面了解为防止黑客对系统实施攻击而对系统进行配置与监控所需要的各种知识。为此，我建议每个应用程序开发人员和系统管理员都应该读一读本书。通过对本书的阅读，你将能够对系统的安全问题有一个更加清楚的认识，并且能够懂得如何充分利用Microsoft公司产品中的安全性功能，设计出安全的应用程序。

Doug Bayer

Windows NT 安全主管

前　言

虽然目前介绍安全问题的书籍相当多，但是许多书籍只是介绍一些安全理论方面的知识，或者只是介绍某一种安全手段，即采用某种工具、应用程序或者技术来实现的安全手段。显然，任何完善的安全解决方案不应该只是一种单一的安全手段。所有的安全商务应用程序都要涉及许多工具和许多技术。另外，将任何一个安全解决方案作为一系列安全手段来进行设计、建立和部署是非常困难的，也是不明智的，因为要使各种安全手段之间能够互相进行通信，需要花费大量的时间和费用。

本书的重点是全面而系统地介绍如何使用各种Web技术来建立基于Microsoft Windows 2000的安全应用程序。我们将从头到尾进行全面的介绍，从浏览器到服务器，再到中间软件服务器，最后到数据库服务器，并且再回头进行说明。你会发现，这样的介绍是一件非常复杂的工作，它涉及到许多组成部件，我们的目的是要确保你能够理解各个部件之间如何实现配套运行。为此，本书既是一本参考书，又是一本教材，也是一本内容详实的说明书，告诉你如何通过使用Microsoft技术来设计安全的Web应用程序。我们还将介绍你在建立端对端解决方案时如何对一些问题作出权衡。例如，采用相应的身份验证和身份识别机制，可能会影响应用程序的运行速度。为此，你必须选择正确的技术来满足你的业务需求。

本书的读者对象

本书的读者主要是开发、部署、支持和使用基于Windows 2000的Web应用程序的Web开发人员和管理员。Web开发人员将学习如何预先将安全特性纳入他们的应用程序，而不是在发现安全问题后再添加这些特性。在应用程序的开发过程结束时才添加安全特性，这是人们常犯的错误，这样肯定会损害系统的安全性。此外还可以了解如何解决和处理好系统的性能、速度与安全性之间的平衡问题。Web管理员将能够学习如何安全地配置Web应用程序，如何确定计算机是否处于黑客的攻击之下，如何对黑客的攻击作出反应。

本书的读者将能更好地理解Windows 2000、COM+、Internet Information Services（IIS）和Microsoft SQL Server中的安全功能，并且能够了解大量的基本安全原则。在建立和部署Web应用程序时，这些知识是极有价值的，基于计算机的所有应用程序都需要某种形式的安全特性。

本书的编排形式

本书的编排形式基本上与我们1999年5月在德克萨斯州达拉斯市为企业软件开发人员举办的技术培训班（Tech-Ed）上提出的应用程序安全性论文的形式相同。那是最早公开展示的基于Web的多层应用程序，它运行的是Kerberos代理程序。本书共分为四个部分。

第一部分：安全性概述与安全应用程序的设计

第1章“安全性基础”概述了核心的安全性原则以及安全问题和对安全构成威胁的种类。第

2章“开发安全Web应用程序的过程”介绍如何设计安全的应用程序，并且分析一个示例情景，作为本书中其余相当一部分内容的基础。安全解决方案的设计过程适用于该示例应用程序，因此你可以看到设计过程是如何进行的。安全问题专家可以跳过第1章，但是所有读者都必须阅读第2章，因为这一章是本书其余内容的基础。

第二部分：各种不同的安全技术及其利弊的权衡

第3章到第7章介绍Windows 2000、Microsoft Internet Explorer 5、Internet Information Services 5、SQL Server 7、SQL Server 2000和COM+ 1.0的安全特性和功能。这些内容是必须阅读的。即使你使用这些产品已经有一段时间了，也能够在这些章节中发现一些新的内容。每一章都对产品的安全功能进行了详细的介绍，并且深入说明了每种产品是如何运行的。

第8章“身份验证和授权检查的实际应用”和第9章“个人信息保密、数据完整性保护、核查和不得否认的实用技术”将介绍实际的安全保护技术。这两章的重点并不是介绍纯粹的技术问题，而是讲述选择不同类型的安全技术时如何权衡利弊，以满足第1章中介绍的核心安全要求。权衡利弊时应该考虑到不同安全技术的性能、可扩展性和“可部署性(deployability)”，同时要考虑你选择要满足的安全要求带来的影响以及如何来满足这些要求等问题。

第三部分：实际应用

第10章“建立安全解决方案” 介绍如何使用第3章到第9章讲述的技术和策略来为第2章中规定的情景建立安全应用程序。这是本书中非常重要的一章，因为它解决了多年来人们提出的最常见的问题之一，即如何在整个安全应用程序中安全地传递认证信息。第11章“安全应用程序的故障诊断”讲述建立应用程序时应该解决的一个最重要的问题，即如何对应用程序的结构进行故障诊断。这一章我们将介绍如何读取事件日志的条目，可以用来帮助你查找问题的工具，并且说明一些常见的错误，包括这些错误带来的影响以及如何消除这些错误。

第12章“防止攻击的安全措施” 重点介绍你将应用程序放到Web上去运行时将会产生什么样的效果。这一章是根据你在建立和部署安全Web应用程序并且将它们放到Internet上去时获得的经验来编写的，有些经验是痛苦的。如果你想将应用程序放到Web上去运行，那么你务必要阅读本章的内容。

第四部分：参考信息

第13章“使用ADSI、WMI和COM+进行安全管理” 介绍如何使用Windows 2000中的工具和脚本编程界面，运用Microsoft JScript、Microsoft VBScript和Perl来建立定制的、可远程控制的管理脚本。最后，第14章“Windows 2000中的Kerberos身份验证方式简介”和第15章“关于Windows 2000中的密码技术和证书的介绍”向读者讲述了Windows 2000中的Kerberos身份验证和加密及证书技术。这两章介绍的内容都非常实用，并且读起来非常容易。

关于本书所附的光盘

本书附带的光盘上包含了一些示例代码和各种工具，可以帮助你使用本书介绍的各种工具

来建立基于Web的安全应用程序。光盘中还包含了本书的电子版，它配有本书所没有的6个附录。首先让我们介绍一下附录。

附录A“Windows 2000众所周知的SID”列出了安装在所有Windows 2000计算机上的账户和它们执行的任务。附录B“安全可靠的口令”介绍如何建立安全可靠的和便于记忆的口令。附录C“Windows 2000的默认端口”是一个Windows 2000计算机使用的TCP和UDP端口的列表。对于防火墙管理员来说，这些信息非常重要。附录D“Internet Information Services身份验证技术汇总”列出了IIS 4和IIS 5支持的所有身份验证协议所具备的特性。附录E“与安全性相关的IIS服务器变量”介绍了所有可以用来帮助你开发安全Web应用程序的服务器变量。附录F“安全Web服务器检查表”是著名的“IIS 4安全性检查表”的IIS 5版本。它可以与光盘上的Hisecweb.inf配置文件配合使用。

下面这个表对光盘上包含的工具和文件进行了基本的描述。

工　具	说　明
Hisecweb.inf	这是用于安全Web服务器的安全性配置编辑器模板。你可以按照第3章的说明来使用该模板
KList	Kerberos标记的列表工具
KerbParser	用于Microsoft Network Monitor的Kerberos分析程序
RUAdmin	当你登录时用来提醒你是否拥有类似管理员优先权的一种工具
TPFX2	通过命令行将Secure Sockets Layer/Transport Layer Security（SSL/TLS）证书添加给IIS 5时使用的工具
CryptUtil	一个COM+组件，用于在Active Server Pages（ASP）中生成适合加密的随机数字。包括源代码
RandomGoo	用于MIPS和SH3袖珍PC的Microsoft Windows CE 3.0应用程序，它能够生成随机数据。可用于产生安全可靠的口令
WhatIf	一个DHTML工具，用于确定哪个安全性设置用于支持授权检查特性
WFetch	一个非常容易配置的客户程序工具，其运行特性很象浏览器。你可以配置许多个值，包括身份验证协议的各种要求，SSL/TLS密码和协议，客户程序身份验证的证书类型和代理服务器信息等
TranslateName	执行Active Directory查看的一个工具，用于在各种类型的名字（如与SAM兼容的名字和UPN名字）之间进行转换。它包括C++源代码
Perlscripts	用于维护安全服务器的各种Perl脚本。这些脚本包括： · Attacks.pl 用于分析IIS W3C日志文件，以便找出常见的攻击痕迹 · Buffy.pl 用于分析C和C++源代码，找出常见的有缓存超载运行问题的API · IP.pl 用于向子网络发送ping命令，以便对子网络进行查询。与Network Monitor配合运行 · Parselog.pl 用于分析IIS W3C日志文件，显示所有的特殊的字段 · Pingsubnet.pl 向子网络发送ping命令，查找开放的端口 · Syn.pl 用于分析netstat命令的输出，以便查看SYN信息溢流

(续)

工　具	说　明
	· Scan　这是一个端口扫描工具 · Uptime　用于生成HTML页，以便显示Web服务器正常运行时间的工具
End2End	用于建立第10章定义的示例中端对端应用程序和示例管理脚本的代码。它有4个目录，每个目录均与第10章定义的应用程序中所使用的一个特定计算机相关 00- WebServer： · ExAirConfig.vbs　用于在IIS 5上创建Exploration Air示例虚拟目录 · WebContent　它包含两个文件，用于构成IIS Web站点 01- Middleware： · DBQuery.dll　这是用于实现用SQL服务器进行数据访问的COM+ DLL。这个DLL展示了两种数据访问方法。比较重要的方法是WhoAmI，它返回SQL服务器确定的用户的名字 · Source　它包含用于DBQuery的Visual Basic 6源代码 02- DBServer： · ExAirHR.sql　它包含用于安装ExAir数据库的SQL Server脚本 03- DomainController： · AddUsers.js和Accounts.xml　用于设置Active Directory中的默认用户Alice、Bob、Cheryl和AppAccount · SetDelg.js　用于设置和清除计算机的Trusted For Delegation（可信赖的身份委托）功能

对系统的要求

若要使用本书来进行安全Web应用程序的设计，你必须拥有Microsoft Windows 2000 Server，或者拥有Microsoft Windows 2000 Advanced Server，也可以拥有Microsoft Windows 2000 DataCenter Server。最好应该拥有另一台计算机，运行Windows 2000 Professional或者能够进行基本身份验证的任何Web浏览器。虽然必须有一个内部网（Intranet）来运行示例应用程序，不过即使你没有这样的网络，你也能够理解它的运行情况。

运行本书附带的光盘上包含的实用程序，你不需要任何编程知识（有些脚本编程语言知识，比如VBScript、Jscript或者Perl，对理解本书中的代码段是很有帮助的）。

本书作者介绍

Michael Howard是Microsoft公司的Windows 2000开发小组中的安全特性开发项目经理，主要负责解决Internet安全性方面的问题和安全特性设计最佳方案的制定。以前他曾经担任过Web基础结构安全程序开发的项目经理，负责下一代Web技术的开发，他也是负责Internet Information Services 5的安全程序开发的项目经理，并且担任过Microsoft咨询服务部的安全顾

问。

Marc Levy是Microsoft公司的BizTalk服务器开发小组的项目经理，过去曾经担任过Microsoft Transaction Server和COM+安全特性开发工作的项目经理。

Richard Waymire是Microsoft SQL Server的项目经理，负责Microsoft SQL Server的总体安全特性的开发。

Micbael Howard
Marc Levy
Ricbard Waymire
Redmond, Wasbingtom
May 2000

目　录

第四部分 参考信息

第一部分　安全性概述与安全应用程序的设计

第1章　安全性基础

1.1　为何要开发安全应用程序

大家都知道，如果我们能够友好相处并且做到互相信任，那么世界将会变得非常美好。可惜，这是不可能的。如果你是个商人，试想你能够仅仅依靠信任来“保证”你想要保密的信息(比如商业上敏感的产品设计或者5年业务计划)的安全吗？如果你在医疗机构工作，你能够仅仅依靠信任来保证患者的病历不被篡改吗？如果黑客篡改了医院的数据，指明病人的疾病需要服用大剂量的违禁药物，这将会造成多么严重的后果啊！

不管你是否承认，信任是一种危险而幼稚的想法。而且，抛开一些极端的例子不说，对你的机构的信息或者你在Web上实施的任何攻击如果成功，都会导致你的机构丧失自信心。因此，除了采取有效的安全措施来防止他人恶意使用或者破坏你的应用程序外，别无选择。

今天的Internet与10年前的情况已经完全不同了，对于毫无戒备的卤莽者来说，这是个非常危险的活动领域。如果你用一个醒目的DNS(Domain Name System，网域名系统)名字在Internet上建立一个新的Web站点，再等上几个小时，你就会发现马上有人来探查你的服务器，然后就可能有不明身份的人来攻击你的站点。用隐蔽身份的方法来实现保密的时代早就过去了。“如果我们不告诉别人我们在这里，别人就永远找不到我们”，这种想法完全是异想天开。实际上，你具备的Internet安全知识越多，对你就越有好处。

1.2　安全的定义

所谓安全，就是要保护好你拥有的资产，资产可以定义为有价值的东西。有一个问题非常重要，即如果某种东西没有任何价值，那么就不值得花费财力和精力来保证它的安全。这个问题我们在第2章中还要更加详细地加以说明。

有些资产属于有形资产，具有货币价值，而有些资产则属于无形资产，但是仍然具有货币价值。例如，我们都知道，有形资产(比如库存产品)是必须保护的，因为大家认为它是“具备一定价值的东西”。但是值得注意的是，某些无形资产(比如与你的公司相关的声誉)也是非常重要的。下面是资产的一些例子：

- 经营计划。
- 动产(所有物)。
- 保密的源代码。