RSA PRESS

安全体系结构的设计、部署与操作

循序渐进地实现网络和平台安全

在真实应用场景中学习安全技术

理解入侵检测系统、防火墙、VPN等技术的优势和不足

[美] Christopher M.King Curtis E.Dalton T.Ertem Osmanoglu 著
常晓波 杨剑峰 译

Mc Graw Hill

清华大学出版社
http://www.tup.tsinghua.edu.cn

安全体系结构的设计、部署和操作

Christopher M. King
[美] Curtis E. Dalton 著
T. Ertem Osmanoglu

常晓波 杨剑峰 译

北京·清华大学出版社

安全体系结构的设计、部署和操作
Christopher M. King, Curtis E. Dalton, T. Ertem Osmanoglu:
Security Architecture: Design, deployment and Operations
EISBN:0-07-213385-6

图书在版编目(CIP)数据

安全体系结构的设计、部署和操作/(美)克里斯托弗,(美)道尔顿,(美)奥斯奥哥罗著;常晓波,杨剑峰译.—北京:清华大学出版社,2003.4
书名原文:Security Architecture Design, Development Operations
ISBN 7-302-06229-3

Ⅰ.安...　Ⅱ.①克...②道...③奥...④常...⑤杨...　Ⅲ.信息系统-安全技术　Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2003)第 002255 号

出 版 者: 清华大学出版社(北京清华大学学研大厦,邮编　100084)
http://www.tup.tsinghua.edu.cn
http://www.tup.com.cn
责任编辑: 许振伍
印 刷 者: 清华大学印刷厂
发 行 者: 新华书店总店北京发行所
开　　本: 787×960　1/16　**印张**: 21.5　**字数**: 481 千字
版　　次: 2003 年 4 月第 1 版　2003 年 4 月第 1 次印刷
书　　号: ISBN 7-302-06229-3/TP·3729
印　　数: 0001~4000
定　　价: 39.00 元

译 者 序

随着网络在企业活动中占据越来越重要的位置，企业对信息安全的需求也日益高涨。部署一个可靠的、强大的、可伸缩的、经济的安全体系结构，并能对各种各样的突发事件做出准确、及时的响应，已经成为现代企业的基本需求。

本书是一本介绍安全体系结构的专著。首先，本书介绍了安全体系结构合理的规划和设计过程，其中涉及制订安全策略、标准和指导；通过对信息和用户进行分级来实现访问控制；明确企业的安全要求；安全基础设施的基本设计原理。接着，本书深入介绍了安全体系结构中常用的一些技术。由于这些技术涉及的方面很多，本书不可能对其实现过程做详细深入的探讨，所以只侧重于阐述这些技术的优缺点、应用这些技术的方法学，以及在虚拟案例中的应用。这些叙述也许不能立即解决您的实际问题，但它能起到抛砖引玉的作用。最后，本书还讲述了如何操作和支持已部署的系统，主要涉及如何管理和分析安全事件、如何进行安全管理，以及定期对安全体系结构进行评定的必要性的方法论。

本书的作者都是在安全管理领域有着丰富经验的专家，他们眼光犀利，论述精辟，为对信息安全感兴趣的读者奉献了一本难得一见的好书。

参加本书翻译的人员有：栗庆丰、王维苏等人。常晓波、庄锦军进行了校对工作，最后由杨剑峰对全书做了统稿。

限于译者水平，难免有错误和疏漏之处，恳请读者不吝指正。希望本书能成为您工作中的好帮手。

致　　谢

感谢我可爱的妻子 Shannon 所给予的无限支持。没有你的支持这本书就不会面世。愿你常伴我身边,好人好梦。

感谢我的儿子 Michael 和 Nicholas,努力工作并且坚持到底,梦想就会成真。

感谢 Doreen 给予我的支持,感谢我最热心的追随者 Connie。

——Christopher M. King

感谢上帝,没有他的保佑,任何事情都不可能成功。

感谢我的妻子 Kelly,她用对我的无限关爱和支持满足和丰富了我的心灵。

感谢我的女儿 Kaylee 和 McKenzie,即便此生只能扮演你们父亲的角色,我也满足了。

感谢我的母亲,她是如此慈爱,鞠躬尽瘁——还常以我为豪,但至今仍常问我靠何为生。

感谢我的父亲,是他让我知道了什么是冒险、挑战与梦想。

另外还要感谢 CMK 在专业知识领域给予我的指导。

——Curtis E. Dalton

感谢父亲和母亲给予我的支持。

感谢 Cathy Watson 在我长时间写本书期间一直陪在我身边。

——T. Ertem Osmanoglu

本书的主要作者

Christopher M. King, CISSP——安全实践领导人

第 1 章　商业和应用驱动器(案例研究)

第 11 章　应用程序安全

第 15 章　检查与完备

Christopher M. King 是 Greenwich Technology Partners 公司(GTP)信息安全小组的实践领导人。他在信息安全领域具有 16 年以上的工作经验,特别在量化安全风险、漏洞以及将 VPN、PKI 和 Web 访问控制等最新的安全技术应用于大型商业应用程序方面具有丰富的经验。他是 Information Security 杂志和 Business Communications Review 的正式撰稿人。

您可以通过电子邮件 cking.rsapress@rsasecurity.com 与 Chris King 联系。

Curtis E. Dalton, CISSP——区域实践领导人

第 5 章　安全基础设施设计原理

Curtis E. Dalton 是 GTP 公司的区域实践领导人。他在金融、电信、制造、研发等商业领域具有 13 年以上设计和部署大型的以网络为基础的信息安全解决方案的实践经验,并且在 Network 杂志、Information Security 杂志和 Business Communications Review 上发表了许多文章。

您可以通过电子邮件 cdalton.rsapress@rsasecurity.com 与 Curtis Dalton 联系。

T. Ertem Osmanoglu, CISSP、MCSE、CCNA——管理顾问

第 4 章　应用策略明确安全要求

T. Ertem Osmanoglu 是 GTP 公司安全实践部门的管理顾问。他在检查、设计和实现安全电子商务基础设施方面(包括证书颁发机构、PKI、一般网络和主机安全)具有丰富的经验。Osmanoglu 先生向全球最大的 2000 家企业(Global 2000)中那些主要面向 Financial Services (FSIP)客户的公司定期提供电子商务策略、风险管理和基础设施咨询。

您可以通过电子邮件 eosmanoglu.rsapress@rsasecurity.com 与 Ertem Osmanoglu 联系。

其他作者

Michael J. Santarcangelo, II, CISSP——区域安全实践领导人

第 2 章　安全策略、标准及指导

Michael J. Santarcangelo, II 是 GTP 公司信息安全实践部门的一名区域安全实践领导人。在加入 GTP 公司之前，Santarcangelo 先生在安德森顾问公司任信息安全实践方面的顾问。在安德森顾问公司期间，他与多个大客户一同设计并实施了安全策略开发解决方案、用户管理系统、Web 平台以及网络体系结构。Michael 具有康奈尔大学的策略分析理学学士学位。

Keith E. Strassberg, CPA, CISSP——高级网络工程师

第 3 章　信息分级和访问控制规划

Strassberg 先生是一名资深的信息系统安全顾问，具有 Binghamton 大学的会计学士学位。Strassberg 先生在 LLP 的 Arthur Andersen 计算机风险管理小组工作期间获得 CPA 资格，在 LLP 他辨出客户 IT 系统中有关操作、技术和商务方面的风险并使风险降至最低。Strassberg 先生 1999 年 6 月加入了 GTP 公司。在计算机安全实践方面的工作中，Strassberg 先生帮助许多客户开发风险评定方法和信息分级系统。

Thomas B. DeFelice, CISSP、MCSE、MCP、MCP + I——高级网络工程师

第 6 章　网络隔离

Tom DeFelice 是一名资深的信息系统安全顾问，在提供网络和系统安全设计服务方面有 13 年以上的工作经验，大多集中在为多个大型多供应商环境解决编址协同工作和安全问题。DeFelice 先生 1998 年 7 月加入了 GTP 公司。在计算机安全实践方面的工作中，DeFelice 先生帮助许多客户设计和开发网络安全设备和报告工具。

Brian Beckwith——高级网络工程师

第 7 章　虚拟专用网络

Brian Beckwith 是 GTP 公司安全实践部门的咨询工程师。他是资深的技术顾问，具有 9 年以上的专业信息系统工作经验，包括网络、开放式系统、信息安全实践和方法学。他具有在大型企业环境工作的丰富经历，对安全外围网络和企业数据通信的细节设计和分析具有深厚的功底。Brian 具有 Rutgers 大学的数学和经济学学士学位。

Richard J. Gondek, CCIE (#5941)、CISSP——高级网络工程师

第 8 章　无线安全

Gondek 先生是一名具有 Fordham 大学企业管理学士学位和 Webster 大学计算机资源管理学硕士学位的安全和网络顾问。他的专业领域包括大型网络设计、外围系统和网络加固，以及网络通信管理、局域和广域的无线网络等新兴技术。Gondek 先生于 1999 年 10 月加入了 GTP，在为公司开发通信新技术和新方法的同时，他还帮助客户解决安全问题，提高客户现有环境的利用率。

David E. Stern, CISSP——网络工程师

第 9 章　平台加固

David E. Stern 是 GTP 公司纽约分公司的高级网络安全工程师。他在校期间成为 ISP/安全设备开发员后，就沉浸在 UNIX 和网络世界中。他在系统、网络和安全体系结构领域具有丰富的经验，并且擅长渗透测试、平台加固和系统安全分析。David 还是 EMT 的志愿消防员，目前是 EMS Company 的中尉。

Carlos Macedo Gomes, CISSP——高级网络工程师

第 10 章　入侵检测系统

Gomes 先生于 1996 年在德州 A&M 大学获得了计算机工程学士学位。在 90 年代早期，还是一名大学生时，他就开始研究信息系统安全，并且在校园安全事件中作为校园 UNIX 顾问，这些经历对他编写 TAMU Tiger 软件包很有帮助。1996 年，Gomes 先生加入德州奥斯汀的 NetSolve 公司，该公司与圣安东尼奥的 WheelGroup 有密切合作，两家公司联合开发了用于监控 WheelGroup NetRangers 入侵检测系统的 NOC(WheelGroup 公司于 1998 年被 Cisco Systems 收购)，后来发展为 Cisco PIX。Gomes 于 2000 年 2 月加入了 GTP 公司，继续应用详细的 TCP/IP 司法鉴定和分析来解决各种涉及安全网络工具和系统的问题，降低客户风险。

J.R. Carlucci——网络工程师

第 12 章　PKI 组件及应用

Carlucci 先生 5 年多来一直担任顾问职务。他曾协助在客户端和服务器两端设计和部署大型 NetWare 和 NT 的扩大迁移。近来，Carlucci 对 PKI 系统进行了广泛的研究和设计。他于 2000 年 2 月加入 GTP 公司，在计算机安全实践部门设计了 PKI 系统以支持大型 VPN 的实施。

Gene Berkinsky——高级网络工程师

第 12 章　PKI 组件及应用

Gene 在过去 7 年中一直是金融和医药公司的顾问。他具有良好的技术经验。他具有

社会学学位并且有工程管理、运作、系统和安全方面的工作经验。Gene 于 2000 年 4 月加入 GTP 公司，并一直领导大型金融机构中智能卡和 PKI 的测试、设计和实施工作。

Gabriel Ioan——咨询工程师

第 13 章　安全事件的管理与合并

Ioan 自 90 年代早期以来一直致力于各种计算机工程的工作。他曾是许多企业的顾问，但作为技术分析员及负责体系结构设计和风险管理的工程领导人，他主要关注的是企业的数据通信和 TCP/IP 安全、银行和投资方面的电子商务工程。Ioan 在一家 Internet 系统管理和部署公司作为技术体系结构设计员工作了一段时间，于 2000 年 11 月加入 GTP 公司，继续从事客户端设计、部署工作并管理基于 IP 安全的系统。

Steve A. Rodgers, CISSP——首席工程师

第 14 章　安全管理

Rodgers 是一名具有 Southwest Missouri State 大学计算机信息系统学士学位的资深安全顾问。他在 International Network Services 作高级顾问期间获得了 CISSP 认证，并于 2000 年 7 月加入 GTP 公司，领导和支持安全实践。另外，他还协助许多客户进行攻击和渗透测试、高级安全体系结构以及安全策略和标准拓展等方面的工作。

关于 Greenwich Technology Partners(GTP)公司

GTP公司主要对采用了高级 Internet 协议、电子/光学和其他复杂技术的复杂网络进行设计、建设和管理。在构成集成基础设施服务的7个关键技术领域提供技术服务,这些领域包括网络、安全、目录服务、集成、系统工程、性能管理和网络管理。GTP 的客户是大型服务供应商和 Global 2000 的企业。

GTP 的顾问和工程师采用特有的 GTP NetValue 方法,可提供用于管理和提供专业服务的最佳实践和过程的框架。GTP 解决方案的关键元素包括:

客观方法,能够为客户提供与供应商无关的建议,以便根据不同客户的战略商业目标、技术需求和现有网络基础设施来做出最佳技术选择;与在网络设备和软件业处于领导地位的开发商形成战略合作关系;复杂网络专项技术,可满足企业和服务供应商网络建设的要求;奉行专业人才吸收聘用策略,这些人才要在各种高级网络技术领域具有渊博知识,要有丰富的实地操作经验,还要具有主导业界的资历证明与证书。

关于技术审校者

麦格劳-希尔是一百多年来技术书籍的最大出版商之一，有为您带来最权威和最新的信息是我们的自豪。为了保证本书内容的高度准确，我们请了许多顶级专业人士和技术专家就此问题对本书加以评价。

Stephen Beck 是 RSA Security 公司 BSAFE 产品线的全球顾问服务主管。Stephen 于 1999 年加入 RSA 公司，两年多来，建立了一支具有世界上资质最高的安全专业人士的小组。Stephen 在信息系统工业、体系结构、设计、实施和复杂信息系统的开发和提供方面具有 18 年以上的工作经验。在安全工业会议和研究会上他是一名很有号召力的的发言人，他的客户遍及全世界。Stephen 具有 Brown 大学的计算机科学学士学位，并且具有安阿伯密歇根大学的计算机科学硕士学位。

我们对 Stephen Beck 先生的深思熟虑与不吝指正表示由衷的感谢。

前　言

章节组织结构

本书针对应用的生命周期讨论如何正确应用安全技术。由安全技术及其配置所构成的安全性集中解决方案称为安全体系结构。书中的三个案例可增加本书的真实性。案例都来自典型的财富 500 强企业;一个是公司站点,另两个是专用的跨行业的(vertical)应用企业(金融和医疗业)。

本书分为三个部分:(1) 规划和设计;(2) 案例中适当安全技术的应用;(3) 已部署系统的操作和支持过程。如果读者希望对技术章节进行更深入的研究,有许多有关这些主题的详细说明可供参阅。如图 0.1 所示。

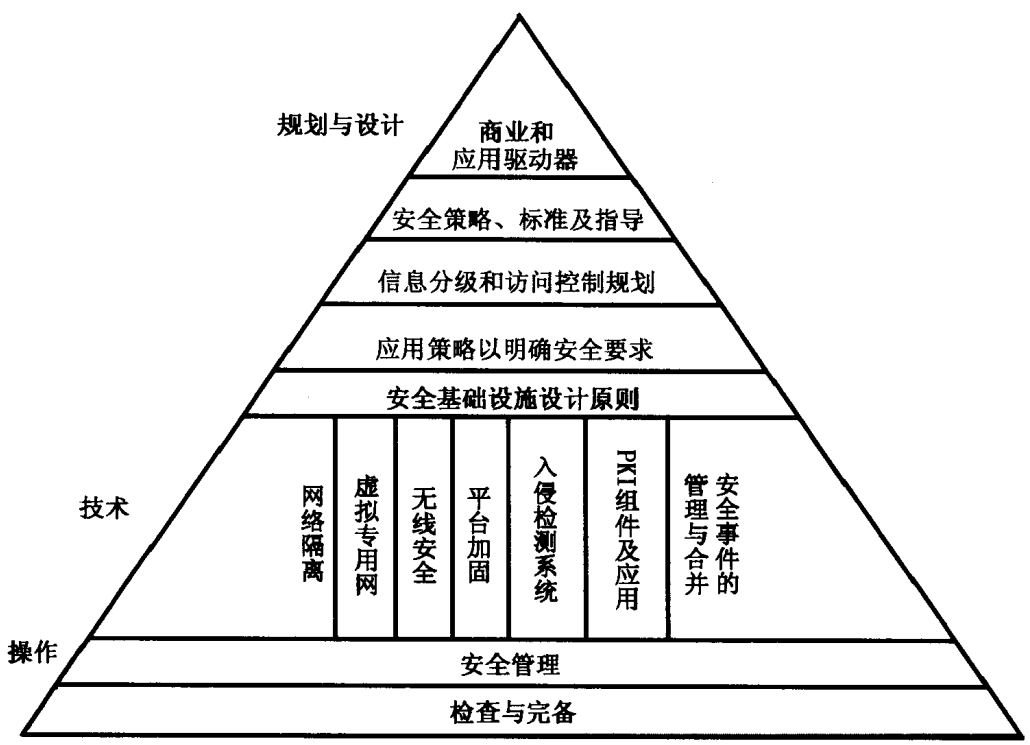

图 0.1　章节结构图

图 0.2 描述了典型的应用程序生命周期。所有的应用程序都开始于解决特定问题的想法。这些想法写在需求定义文档中，文档由高级管理人员评估后通过。然后设计和编写应用程序。这可以是一步或两步过程(先设计，而后获得通过，然后开始编写)。一旦应用程序通过评估，它必须放入基础设施内。基础设施的任何变化也都必须经过评估。当应用程序放入基础设施后，可进行安全评定，以验证不会引发更改及排除不安全因素。如果没有发现安全漏洞，此应用程序就可进入生产环节，应用程序生产出来后，只需要技术支持就行了。

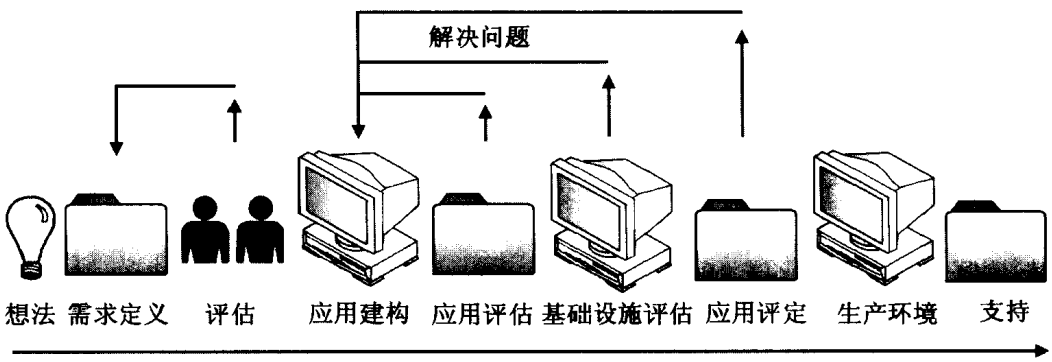

图 0.2 解决方案生命周期

规划与设计

最好的解决方案以详细的规划和设计阶段为起点。这样有利于降低建构和测试阶段工作的复杂程度。在目前快节奏的 IT 行业中，规划和设计的时间常常被缩短，以满足“面市时间”的限制。

第 1 章 商业和应用驱动器(案例研究)

本章定义了用来解决特定商业问题的商业应用程序。本章所述的三个案例将在本书后面的各个章节中引用。本书组织结构图中的各个主题都将利用这三个案例来分析和处理。

第 2 章 安全策略、标准及指导

安全策略构成了所有良好安全体系结构的基础。本章讨论策略、标准及指导的区别，以及由跨行业的行业(与金融或医疗保健相关的)所决定的可应用的规章需求。

第 3 章 信息分级和访问控制规划

为证明安全控制适当，需要评估数据的有形价值和无形价值。数据必须按照丢失、声誉、竞争力、数据缺失和可用性等方面的风险划分为适当的级别。用户的角色和责任必须在适当的访问控制规划中进行定义。

第 4 章 应用策略以明确安全要求

本章将安全策略和调整说明具体为三个案例的特定安全需求。安全需求根据安全服务(机密性、完整性和可用性)进行分类。根据数据所需的处理类型,部署特定的访问控制机制(如认证、授权、审核和管理)。

第 5 章 安全基础设施设计原理

开发出能满足所有安全需求并能抵抗任何可能攻击的安全基础设施,这是一种艺术与科学并进的能力。本章介绍在安全部署中通用的基本设计原理。

安全技术

安全技术不应中断商业过程。每个技术章节都包括所需背景资料部分、如何使用技术的方法学部分以及与案例有关的应用部分。

第 6 章 网络隔离

保护敏感应用程序的第一道防线是对网络进行分割。网络中的流量只应该来自可信平台。与不可信平台和网络(如 Internet 和 Extranet 合作伙伴)的直接连接是十分危险的。本章讨论了高可用性技术、多种网络接口,以及基于主机的平台和专用设备平台。

第 7 章 虚拟专用网络

更快的接口和 Internet 连接点的迅猛增长促进了 VPN 技术的发展。安全共享公共网络的能力明显降低了专线的费用,并提高了传统拨号访问的速度。但这种相对较新的技术也带来了很多挑战。

第 8 章 无线安全

以无硬件连接的形式随时随地按任何方式访问信息,这种能力是无线网络最吸引人的地方。但是,无线网络与有线网络相比,面临着更大的安全挑战(如窃听、哄骗和拒绝服务)。

第 9 章 平台加固

保护敏感应用程序的第二道防线是加固平台。编写不良的应用程序或脆弱的网络控制将使平台暴露在非授权用户面前。透明的没有安全措施的操作系统会产生许多默认用户账户并向他们提供不必要的网络服务。加固平台的惟一方法是使用应用程序(如 Web 服务器、数据库或应用程序服务器)对平台进行测试。

第 10 章 入侵检测系统

为充分监控系统、主机或应用程序，必须使用入侵检测系统。防火墙、平台和应用程序日志会生成大量对检测人员无用的信息。IDS 可对攻击信号进行匹配以实现异常识别。

第 11 章 应用程序安全

在 Internet、外部商业合作伙伴以及远程访问流量多个连接的情况下，传统网络平台上的安全控制装置已经无法对敏感资源提供必要的访问控制精度。这样的基础设施不适合保护内部应用程序的功能和数据。必须要确保应用程序只用于预定目的，且只被适当的用户使用。应用层安全是在应用程序内部实施访问控制原理，以阻止和侦测未授权的访问。

第 12 章 PKI 组件及应用

公钥基础设施(Public Key Infrastructure，PKI)是一组组件和规程，通过数字证书管理支持加密密钥。支持 PKI 的应用程序可以提供认证、数据完整性、机密性和不可否认安全服务。该技术在信息安全领域已经成为许多问题的解决方案。本章介绍其在案例中的优缺点及应用。

操作和支持

安全体系结构的规划、部署和配置已经完成。在实践中，安全体系结构组件不会自动暴露(开放)。暴露的主要原因只在于人们的错误(组件错误配置)。本章讨论了如何管理安全组件、用户管理和安全事件的发生。最后，讨论组织机构测量其安全体系结构的方法和最佳商业实践。

第 13 章 安全事件的管理和加固

安全组件可以生成非常精细的安全事件日志。在体系结构中的战略地点，使用的设备越多，每个设备为描绘此环境的清晰画面所提供的细节就越多。所有安全事件的实时协作和相关性可为正在进行的攻击提供可靠的证据。

第 14 章 安全管理

安全管理员管理网络、平台和应用程序的安全配置。用户管理通常不在安全管理员的管理范围之内，而属于拥有此应用程序的公司部门或公司的帮助桌面。本章讨论与管理企业环境和应用程序管理有关的方方面面。

第 15 章 检查与完备

安全体系的规划、部署和运作过程位于其生命周期的末端。任何系统的安全控制都应该与相应的业务风险相匹配。安全评定能够确保安全体系结构达到甚至超过安全策略和最佳商业实践。安全完备模型允许机构根据行业最佳商业实践测量安全体系结构并在业务中加以应用。

序　二

最近信息安全受到了广泛的关注，这是因为目前大部分商业组织都已经与 Internet 和万维网相连。现在，对于大多数高级企业主管而言，安全问题不再遥不可及了，而是已经开始在自己身旁发生。安全漏洞会大大降低公司的市场价值，甚至威胁企业的生存。即使最小的漏洞也能将公司的名誉、客户的隐私信息和知识产权置于危险之中。还有成功的攻击对于企业官员将造成严重的个人损害。1996 年颁布的国家信息基础设施保护法令（National Information Infrastructure Protection Act）规定企业官员必须对因重大疏忽造成的损失向股东承担责任；根据此项法律，公司必须在保护企业资产方面显示其应有的能力。

针对这些风险，有人可能会认为在大型企业中部署有效的安全基础设施是一件简单的事情。不幸的是，这种观点是错误的。出于各种原因（尽管不充分），许多企业都缺乏有效的安全检测机制。部署可靠的安全基础设施不仅复杂而且耗费巨大，因为安全在根本上既需要横向的实践，也需要纵向的（普遍）实践。在网络连接、系统和网络管理方面有许多重叠的地方，而且，安全环境也在不断发生着变化。安全原则必须能跟上飞速发展的应用程序开发技术。基于 Web 的应用程序环境越来越分散（因为进程分布在不同的 Web 服务器、应用程序服务器、企业 JAVA bean 和数据库上），按分布式体系结构的形式提供访问控制是一个巨大的挑战。这些问题不会随着时间的推移而消失。新的技术、应用程序和平台不断开发出来（速度和功能都在不断攀升），安全防卫永远滞后于技术的飞速发展。

而且，描述部署安全基础设备的成本投资回报率（ROI）也是一项巨大的挑战。在评估 ROI 时，安全风险（和费用）必须与企业风险（和费用）一起考虑；这在许多公司通常需要经过大量的努力。尽管安全暴露问题引发了公众的广泛注意，但是许多企业的反应很慢，甚至没有任何反应：除非漏洞的影响可以映射成企业内特定的风险，否则企业仍然不愿意增加防卫措施和建立大规模（昂贵的）安全专家队伍。

在这样的环境中，企业如何才能有效地解决这些问题呢？一种方法是部署外包的解决方案，如管理防火墙、远程访问许可和远程安全事件监控。但是将企业资产的保护交给第三方会有很大风险，因为外包的解决方案通常仅能用于保护公司的外壳（边界）。一旦边界被攻破，黑客就可以轻易地获得资源和敏感数据，因此外包解决方案虽然有效，却不能解决所有挑战。

值得高兴的是，已经有一些方法可以帮助企业建立安全灵活的基础设施，并保护极其复

杂的应用程序和资源。通过应用本书讨论的适当的安全技巧(规划、在不同级别部署访问控制机制、监控等),企业可以在面对未知敌人时有效(且低成本)地保护自己。

Johna Till Johnson
高级副总裁
首席技术执行官
Greenwich Technology Partners
2001 年 6 月