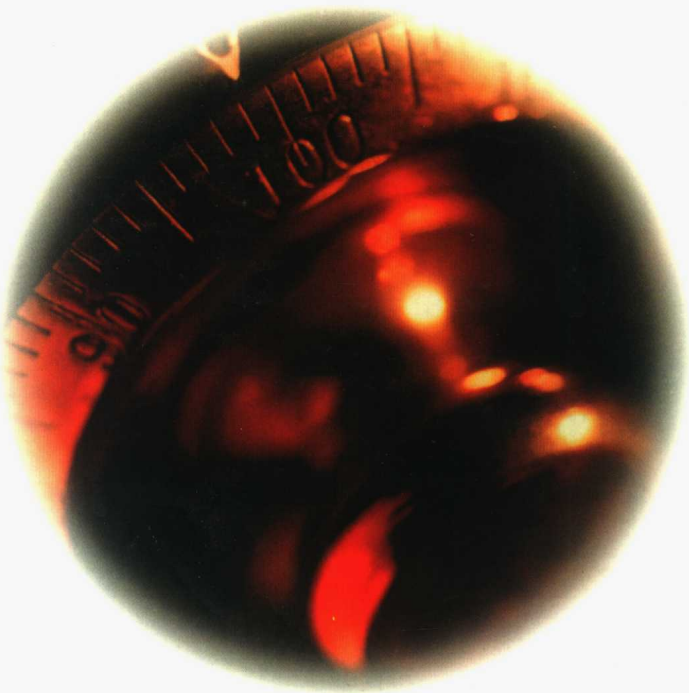
Mastering Web Services Security

全面掌握 Web 服务安全性



(美) Bret Hartman
Donald J.Flinn 等著
杨 硕 译

清华大学出版社

全面掌握 Web 服务安全性

(美) Bret Hartman
Donald J.Flinn 等著

杨硕 译

清华大学出版社

北 京

内 容 简 介

本书讲述了用于保护 Web 服务的各种技术。内容涵盖 Web 服务安全的各个概念，由浅入深地介绍了 XML 安全、WS-Security、SAML 等基础内容，以及用于保护 Web 服务基础结构、.NET Web 服务、Java Web 服务的安全技术和 Web 服务体系结构的实现方案。

本书引入众多新的安全技术，内容全面翔实、浅显易懂，适合各类人员的学习。

Bret Hartman Donald J.Flinn et al.
Mastering Web Services Security
EISBN：0-471-26716-3

图书在版编目(CIP)数据

全面掌握 Web 服务安全性/(美)哈特曼(Hartman，B.)等著；杨硕译.
—北京：清华大学出版社，2004
书名原文：Mastering Web Services Security
ISBN 7-302-08642-7

Ⅰ.全… Ⅱ.①哈…②杨… Ⅲ.互联网络—安全技术 Ⅳ.TP393.48
中国版本图书馆 CIP 数据核字(2004)第 044452 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：曹康
文稿编辑：侯彧
封面设计：康博
版式设计：康博
印 装 者：北京昌平环球印刷厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：22.5　**字数**：576 千字
版　　次：2004 年 6 月第 1 版　2004 年 6 月第1 次印刷
书　　号：ISBN 7-302-08642-7/TP·6197
印　　数：1～4000
定　　价：43.00 元

序

本书的基本前提是要求 Web 安全服务的应用程序能够使用统一的安全体系结构。身份验证、授权、责任、管理和密码术安全服务都可以通过一个轻便、健壮，并对所有已经定义的应用程序通用的体系结构来提供。

这是一个令人生畏的概念，但它能发挥很大的作用。

在 Credit Suisse First Boston(CSFB)，我们已经实现了 EASI(企业应用程序安全集成)统一安全体系结构。在近一年半的时间里，我们认真记录了自己的需求，而根据需求制订出了对应的规范。2002 年，我们实现了 EASI 统一安全体系结构，认真测试并验证每一个 API、映射表和组件。2003 年，这个体系结构被指定为开发新应用程序的标准，允许我们复用已有的安全服务，从而减少开发时间和开发成本。

对于 EASI 架构，我们抱有很高的期望。在 Credit Suisse 中，Web 服务得到了广泛使用。只要用户能够设想出 Web 服务的工作方式，我们差不多就可以在 CSFB 中以相同方式使用。在查看任何类型的架构时，灵活性、实现方式的简化和健壮性对于用户来说都很重要。同样，国际管理和审计需求也迫切要求用户寻找标准化和减少复杂性的方法。

像所有真正令人生畏的概念一样，进行复杂且无法避免的“范式修改”非常必要。对于管理伴随实现的不同类型的文化变迁和挑战来说，应该有专门针对这方面的特定书籍来阐述。过去我们在 CSFB 中应用的方法是创建一个强大的跨部门小组，来协调工作、监控进度和处理问题。

最后，我认为实现这样一个统一的体系结构是必然的。任何不顺应这种趋势的行为都是没用的。目前，为每个开发的应用程序重新定义一个安全的解决方案空间不再是可行的。简单地说，对于有限的支持资源来说，产品环境已经变得过于复杂。要维护安全和信任几乎是不可能的，因为应用程序必须跨越旧式大型机和现代的客户/服务器环境，并且它们还有已知的但每天都在更新的安全漏洞。EASI 体系结构把这个环境简化为已知的、安全的和可信的组件。

同样，用户可以延长旧式应用程序的生命期。旧式安全服务的退出与新式安全服务的集成都可以不重新编写应用程序。

软件公司已经懂得上述这些概念的重要意义。Microsoft 公司推出了.NET Framework，Sun 公司推出了 Sun ONE，并且都承诺它们的产品提供了通用的安全体系结架构构，这表明了它们对这些概念的理解和欣赏。在CSFB中，我们将EASI体系结构作为基础，而且把.NET和Sun ONE集成到 EASI 中。

我相信您会逐渐赞同本书提出的理念。我可以以个人名义担保我所了解的事实：为了撰写本书，作者牺牲了很多周末休息时间。Bret 和他的小组时常会在又一个周末的劳作后睡眼矇眬地出现在 Credit Suisse，尝试完成本书的撰写、修改和编辑。

当 Bret 请我为该书写序言时，我个人感到非常荣幸……但并不是因为您最初猜想的原因。

我们的交情不错，自从发现我们在剑桥大学最有竞争力的两个学院学习就开始了，所以我

不愿放弃这个机会。

Bret，虽然您和小组的绝大部分成员都是 MIT 的毕业生，但是我希望引用安娜•弗洛伊德的话来表达我的想法：

“具有创造性头脑的人总是能够战胜任何糟糕的状况。”

John Kirkwood
Director，Global Security Strategy and Architecture
Credit Suisse First Boston

引　言

Web 服务是一种很有前途的解决方案，它可实现客户和企业之间快速而灵活的信息共享。Web 服务能够访问那些以前被锁定在公司网络内部并且只能通过专用软件来访问的数据。Web 服务在为我们带来好处的同时也引发了一个严重的风险：敏感的、保密的数据可能会泄露给那些不应该看到的人。在我们学会如何处理 Web 服务的相关风险后，Web 服务才能释放它们巨大的潜能。

Web 服务代表分布式计算的下一个发展阶段，它们建立在以前的分布式模型基础上。分布式计算的推广源于 Transmission Control Protocol/Internet Protocol(TCP/IP)协议。对于那些只想建立业务应用程序的编程人员来说，使用 TCP/IP 建立分布式产品是一项艰巨的工作。为了减轻分布式编程的负担，计算机业内首先开发了建立在客户机/服务器计算范式基础上的 Distributed Computing Environment(分布式计算环境，简写 DCE)，随后又开发了 Common Object Request Broker Architecture(公用对象请求代理程序体系结构，简写 CORBA)。与此同时，Microsoft 引入了 Component Object Model(组件对象模型，简写 COM)，后来又引入了以 DCE 技术为基础的 Distributed COM(分布式组件对象模型，简写 DCOM)和 COM+。Sun 在其 Java 语言的基础上引入了 Java 2 Platform，Enterprise Edition(Java 2 企业版，简写 J2EE)和它的通用 Enterprise Java Beans(EJB)，它们采用了以往技术中的很多概念和研究思路。上述的每一次发展都使分布式计算变得更加简单，但是这些技术都是相互孤立的，要在不同的中间件技术之间实现互操作性是很困难的。

现在 Web 服务已经得到蓬勃发展。Web 服务有两个主要目标——使分布式计算对于业务编程人员来说变得更加简单和增强互操作性。下面的因素可以帮助实现这两个目标：

- 请求程序和服务提供者之间的松散耦合
- Extensible Markup Language(可扩展标记语言，简写 XML)的使用，它是平台和语言中立的

如果顺利的话，在 Web 服务模型中将会保留以前分布式模型的所有优点。

在实现所有那些过去的分布式模型的过程中，一项技术(即安全)似乎总是在最后才被考虑。好像这里存在一句咒语，“首先使模型运转起来，然后再考虑安全”。不可避免地，这导致了性能拙劣和难以使用的安全。众所周知，分布式计算的安全是一个令人头疼的问题。

我们到底从以往的经验中汲取了哪些呢？首先，我们目前正处于 Web 服务的初级阶段，我们为您提供了一本主题是将分布式安全概念应用于 Web 服务的书。在这本书中，我们具体介绍大量规范组和厂商的工作，它们正在处理和 Web 服务基本技术(XML 和 SOAP(简单对象访问协议)相关的安全问题。所以，我们已经汲取了过去的经验。然而，您将看到，在我们描述 Web 服务安全的同时，Web 服务安全模型中仍然存在一些限制，部分模型还不能完全协调地工作。

几乎每天都会看到新发表的文章，声称假如没有安全，Web 服务将不会成功。我们希望本

书能够传播 Web 服务安全所需的东西和目前所缺失的东西。希望本书能够帮助您在 Web 服务的分布式应用中开发自己的安全解决方案。

把 Web 服务安全限制在公司的周边防火墙范围内是不够的。在当今的电子商务世界中，客户、供应商、远程雇员，有时甚至是竞争对手都被邀请进入您计算系统的内部区域。因此，使用 Web 服务范式的分布式安全需要端对端的安全——一个服务请求发出后，它将通过周边防火墙，进入应用程序服务器和公司网络核心部分的应用程序，然后到达后端保存机密数据的永久存储器中。随着本书的介绍，您会明白 Web 服务已经深入到许多由 Web 服务引起的新型体系结构设计中。因此，本书将使用理论、示例和有实际意义的建议向您介绍如何保障企业端对端的安全。

端对端电子商务的基础是更为宽泛的分布式计算技术和各种分布式安全技术。计算领域的每个人和许多典型的计算机用户都曾经听说过 Hypertext Markup Language(HTML)和 Secure Sockets Layer(SSL)，但是很少有人了解 EJB、COM+或者 CORBA。然而这些技术却位于现代分布式计算系统的核心部分，这些计算系统则处于周边防火墙之后。这个区域被称作中间层，它是端对端的企业安全中最复杂的区域，也是最容易忽视的区域。近期的一些政府调查显示，中间层最容易被非法闯入，从而导致巨额的财政损失。在电子商务活动的驱动下，越来越倾向于让外部人员进入中间层，这样中间层变得更容易非法闯入，从而导致更大的财政损失和隐私侵犯的潜在威胁。

如果您对您的站点的任何一部分负有安全责任，不管是直接的或者是间接的，都应该阅读和学习本书。分布式安全并不是一个简单的主题，而 Web 服务安全又额外增加了一层复杂性。因此，本书这些部分的内容并不简单，但是如果您掌握了这个复杂的主题，那么您和您的公司将获得显著的回报。

本书提供一些相关材料，介绍如何使用体系结构和技术，以及如何理解建立一个安全的 Web 服务系统的规范。考虑到当前技术正在快速发展，我们还将提供模型背后的理论，并解释隐藏在许多处于当今技术前沿的安全规范之后的思想。之所以安排我们来完成这本书，是因为本书的作者都是编写这些规范的委员会或组织的成员，同时也正在从事设计和建立企业安全产品的实际工作。

本书的重点在于向您展示如何建立安全的端对端 Web 服务系统，以及怎样理解这个系统的复杂性。因此本书中将不会深入涉及安全的一些晦涩难懂的方面，例如密码术、公钥基础结构(Public Key Infrastructure，简写 PKI)以及如何建立中间件系统等。然而，本书将从如何在 Web 服务系统中使用这些专用的安全技术的角度来讨论它们，帮助您理解它们的特性，从而使您能够判断最符合自己需要的方案。

本书不仅将在技术上帮助您理解端对端企业安全体系结构的主要组成部分，还将在宏观上描述如何配置和使用 Web 服务安全技术，从而来保护您的企业和它与外部世界的交互作用。

0.1　本书概述和技术概况

企业安全就像一场正在进行的战斗。战斗的一方是那些想要侵入您的系统的人，他们或者是为了获得乐趣，或者是为了能够给自己或者他们的组织牟取利益。战斗的另一方是那些像您

一样采取防御措施阻止外部非法侵入者。这场持续的战斗导致了安全解决方案也在不断变化。当前正在发展的一组安全要求是致使安全解决方案不断变化的另一个因素，例如为了电子商务的目的，给予一组陌生的外部人员有控制的访问您的系统的权利。考虑到以上原因，本书将着重解释当今企业安全解决方案背后的基本思想，从而使您不仅能够在遇到新型解决方案的时候判断它的价值，还能够判断旧的解决方案何时不再适用。

对 Web 服务的一个重要要求是支持在底层对象模型之间的安全互操作，例如.NET 和 J2EE，同时还应支持在周边安全和中间层之间的互操作，以及在中间层和旧式系统或者后端系统之间的互操作。因此，本书将具体描述维护安全互操作性过程中存在的问题，而且还将指导您如何去克服这些问题。由 Organization for Advancement of Structured Information Standard(结构化信息标准推进组织，简写 OASIS)、World Wide Web Consortium(万维网协会，简写 W3C)和 Internet Engineering Task Force(Internet 工程任务组，简写 IETF)组成的分布式安全组，已经在规范中对存在的部分问题提供了解决方案，这些规范是由分布式安全组的成员公司合作开发的。其他组织，例如 Web Service Interoperability Organization(Web 服务互操作性组织，简写 WS-I)和 Java Community Process(JCP)，已经致力于补充解决方案的工作。本书中这些内容都将涉及到，从而为读者提供中肯的分布式安全操作和思想。

我们不仅从端对端企业角度来解决安全问题，与此同时还将从身份验证、授权、安全传输和安全审计这些主要的技术角度来解决安全问题。从这 2 个角度来描述企业安全，本书将采用由上至下和由下至上这 2 种方式来帮助您理解存在的安全问题和相应的解决方案。

在某些情况下，不存在标准的解决方案。本书将为您提供最新的思想和指导，从而帮助您能够在这种情况下获得适当的解决方案。最好的解决方案是在开放的标准下产生的，这是因为解决方案将通过严格的检查和安全专家的讨论，以便达到标准状态。然而，标准化是一个缓慢的过程，而我们面临解决问题的压力。在还没有达成一致的情况下，我们提出自己或者其他人过去已经实现的解决方案，然后描述在分布式安全群体中讨论的各种可能的解决方案。

本书尝试着在理论和对 Web 服务安全的理解间寻求平衡，以便能够帮助您决定使用当前方案的时机，以及应该在何时放弃不完善的解决方案，进而寻找一个更好的解决方案。正像一句谚语所说的，与其施舍给一个人当天的膳食，不如教会他如何耕种。这也是本书试图遵从的原则。我们期望您从本书中学习的知识有助于您建立安全的系统，随时应对将来出现的新的解决方案、需求和威胁。

如果您读过我们以前写的书，“Enterprise Security with EJB and CORBA”(Hartman，Flinn 和 Beznosov 于 2001 年编写)，您会注意到本书中的一些观点和文字出自该书，而且在本书中得到了更新。例如，企业应用程序安全集成(Enterprise Application Security Integration，简写 EASI)概念就是对前面书中曾经讨论过的企业安全集成(Enterprise Security Integration，简写 ESI)概念的升华。本书关于 Web 服务安全的内容是前面书中观点的自然演变，因为我们相信应该从整个企业安全体系结构的环境中来查看 Web 服务安全。虽然还有很多新技术值得去讨论，但是建立企业安全体系结构的基本原理是相同的。

可能您会注意到在不同的章节之间，写作风格和侧重点都有所不同。这是因为本书有 4 位作者，我们拥有不同领域的安全专业知识，认为需要考虑的最重要的问题也都各不相同。我们尽力保持在正文中术语的一致性，但是由于本书涉及到很多复杂主题，因此在书中出现一些变

更是不可避免的。我们希望我们各自不同的观点能够为您所用，为您提供几种不同的考虑 Web 服务安全解决方案的方式。

0.2 本书的组织结构

本书分为 3 个部分，如下所述：

- 第 1 至 3 章提供对 Web 服务和安全问题的基本介绍，帮助您了解其基本知识。如果只是确保非常简单的 Web 服务应用程序的安全，这一部分将提供您需要的所有信息。第 3 章描述了一个使用.NET 的 Web 服务应用程序，其中.NET 可以提供有限的 Web 服务安全，而不必去开发任何安全代码。
- 第 4 至 7 章中详细描述了 Web 服务安全的技术构件。这些章节定义了支持 Web 服务安全的安全技术，着重强调了安全技术与 XML 是如何协同工作的。对于那些希望了解 Web 服务安全和支持基础结构技术，但却不一定关心安全应用程序是如何建立的人来说，这些章节会引起他们的兴趣。
- 第 8 至 12 章是本书最后一部分，在这一部分中具体介绍在建立应用程序时，如何应用 Web 服务安全。第 8 章和第 9 章将描述在最普通的应用程序平台，即.NET 和 J2EE 上实现 Web 服务时可以使用的功能。后面的章节中将介绍互操作性、管理和集成这些高级主题。本书的最后一章是描述如何计划和实现一个完整的安全体系结构，在这一章中会用到前面学过的所有概念。

第 1 章的内容主要是介绍 Web 服务安全的主题，以及用来解决 Web 服务安全问题的新技术。这一章将为理解接下来的章节如何融入整个解决方案打下基础。第 1 章中还引入了风险管理的概念，通过它使得在系统性能与复杂性和受保护的资源价值之间达成平衡。另外，我们还介绍了企业应用程序安全集成概念，而且还介绍了它是如何支持端对端企业安全的。在第 1 章的结尾部分对本书中虚构的企业，即 ePortal 和 eBusiness 作了描述，在贯穿本书后面部分的一个运行示例中将会用到这 2 个虚构企业。

第 2 章开头部分详细描述了 Web 服务以及它们可以为分布式计算带来的好处。接着又介绍了 Web 服务的语言——XML，然后是基于 XML 的消息协议——SOAP。在描述了 SOAP 之后，本章又介绍了可从 Web 访问的 Universal Description，Discovery，and Integration(UDDI)服务，可以用它来发现 Web 服务，从而使请求者能够与服务通信。在这一章中描述的下一个组件是 Web 服务描述语言(Web Services Description Language，简写 WSDL)，这是一个基于 XML 的，由计算机生成的并可由计算机处理的文档，此文档详细描述了如何访问一个 Web 服务。通常，在读者开始对互操作性感兴趣时，也就产生了对标准和标准组织的需要。第 2 章介绍了在 Web 服务领域工作的重要标准组织。

第 3 章介绍了作为 Web 服务安全基础的安全技术。这一章将介绍密码术、身份验证和授权的基本原理。这些技术是自然发展的。最基本的是底层的密码术，其次是使用密码术的身份验证，然后是授权，它依赖于经过身份验证的主体。接着，描述如何使用这些安全技术来实现一个简单的 Web 服务，将用到前面第 1 章引入的 ePortal 和 eBusiness 示例。这个简单的示例仅使用 Web 服务的一项技术，即.NET。可以使用基本的安全措施来保护一个简单的系统，而 Web

服务通常需要更为复杂的安全措施。本章将讨论那些基本方法的局限性，而且在本书后面部分将描述一组完善的安全技术，这些技术是企业部署所必需的。

第 4 章主要讨论确保 XML 和 SOAP 消息安全的措施。因为这些措施中的大多数都建立在密码术基础上，所以本章将描述公钥密码术，并介绍它的适用范围，除此之外本章还将讨论数字签名和公钥基础结构(PKI)。在第 4 章中还将概述一些应用得更广泛的公共加密技术，例如 RSA、Diffie-Hellman 和 DSA。本章中还会介绍公钥证书，它是在公钥中建立信任的一个必要因素。在此之后，本章将介绍加密和数字签名是如何在 XML 文档中应用的。最后，本章讨论这些措施是如何按 SOAP 和 Web 服务定制的，而且还将介绍用来确保 SOAP 文档安全的 WS-Security 规范。

第 5 章主要讨论 Security Assertion Markup Language(安全断言标记语言，简写 SAML)规范，这个规范使用 XML 来确保基本证书的安全。这一章将描述 SAML 通常的用法，以及如何与 Web 服务联合使用。这一章还将具体介绍适用于各种不同 SAML 断言的规范，以及它的请求－回复模型。此外，本章还会介绍 SAMLbrowser/artifact 配置文件的单点登录(SSO)方法以及 SAML 是如何融入一个更大的体系结构的。我们描述分布式 SAML 管理机构，它们执行身份验证、属性检索、授权这样的安全功能并且介绍访问这些机构的协议。本章还会介绍 SAML 断言的应用程序间传输协议。本章通过研究一个 Shibboleth 项目，给出一个基于 SAML 的解决方案的示例，用于解决隐私，SSO 和联盟问题。

第 6 章集中介绍了几种前面定义的安全技术，并将其放在第 1 章介绍的 Web 服务示例的环境中进行描述。我们把这个安全解决方案分为面向连接的解决方案和面向文档的解决方案，具体分析可能的安全解决方案，确定它们如何适应 Web 服务安全。在讨论了基于 XML 的 SOAP 消息在两个域之间进行通信的安全之后，我们研究身份验证、授权和在 Web 服务接口上的数据保护，而且还将描述 WS-Security 和 SAML 规范之间的关系。由于 Web 服务是新生事物，目前还没有公认的最优方法，所以本章将分析 Web 服务安全需要，并确定如何满足这些需要。

第 7 章概述了用于创建 Web 服务应用程序的不同中间件技术中的安全问题。在概述中讨论了中间件、客户-服务器和对象范式，它们是现代分布式体系结构的基本构件。接着，又讨论了身份验证、消息保护、访问控制、信任、管理和细粒度访问控制的分布式安全基本原理。然后又解释了用来建立 Web 服务应用程序的常见分布式中间件技术 CORBA、COM+、.NET 和 J2EE 的安全机制。

第 8 章描述了如何使用 Microsoft 技术来实现安全的 Web 服务。这一章介绍了使用 COM+、带有 SOAP 工具包的 COM、.NET Remoting 和 ASP.NET 来创建 Microsoft Web 服务应用程序的不同方式。接着，本章又阐述了确保基于 ASP.NET 的 Web 服务安全可以使用的机制——它是在 Microsoft 世界中开发互操作式 Web 服务的最灵活也是最有效的方法。我们使用示例 eBusiness 和 ePortal，同时结合 ASP.NET 来阐释基于 ASP.NET 的 Web 服务的安全。

第 9 章描述了当目标 Web 服务是一个 J2EE 应用程序服务器或者 Java 应用程序时，如何确保 Web 服务的安全。我们将会了解致使 Web 服务安全区别于传统的 EJB 安全的原因，以及读者如何在 Web 服务环境中确保一个 J2EE 容器的安全。自始至终，我们都要参考那些 JCP 正在开发的和已经开发的新 JSR，以保证 Java 与 Web 服务能够兼容。接下来，本章要使用 eBusiness 和 ePortal 示例来阐释如何使一个传统的应用程序服务器能感知 Web 服务。我们引入了 Systinet

的一个产品，它为应用程序服务器提供了一个 Web 服务开发平台，而且讨论了与这个方法有关的安全问题。我们还使用 Sun 公司的 Java Web Service Developer Pack(Java Web 服务开发者包，简写 JWSDP)开发了相同方案。

第 10 章讨论了 Web 服务实现——这些 Web 服务建立在不同应用程序平台上并运行在不同策略域——之间实现互操作性的困难之处。在这一章中，我们将了解 Web 服务的不同安全规范，同时还将指出在安全互操作性的某些领域，这些规范存在的局限性，例如联盟和委托。本章将列举并描述在 Web 服务领域使用的很多安全工作，还将展示如何一起使用 SAML 和 WS-Security 来保护 Web 服务消息的安全。除了在约束很多的情况外，我们认为当人们试图在 Internet 上使用 Web 服务时，当今可以使用的安全技术仍缺乏很多重要功能。本章的结论是 Web 服务将首先在 Intranet 中使用，然后扩展到 Extranet，最终当 Web 服务安全组织解决了在这些领域中的问题之后，Web 服务才能够扩展到在 Internet 上使用的应用程序。

第 11 章从底层中间件的安全的角度描述 Web 服务的安全管理，还将讨论 Web 服务数据保护方法。本章的开头主要讨论了安全管理的基础、安全属性对主体的分组、Role Based Access Control(基于角色的访问控制，简写 RBAC)模型的使用，以及如何在 Web 服务中使用它们。RBAC 在访问控制中很实用，但是在管理基于 RBAC 的系统时，存在很多困难和缺点，本章将对其进行介绍。我们讨论委托的管理，同时也指出这种方法的风险以及认真指派委托的必要性。在复杂系统的访问控制中使用风险管理时，我们建议把审计作为安全系统必备的一个部分。本章的结尾部分讨论在 SOAP 消息中进行数据保护管理。

第 12 章使用一个安全部署 Web 服务业务方案的实例来总结前面章节中介绍的理论和方法。在这一章中，我们会向您展示 eBusiness 和 ePortal 示例的实际计划和部署过程。本章指出了许多在部署过程中能够诱惑您的陷阱，并且阐述如何避免它们。通过提出一个实际的方案，描述防火墙、Web 服务器、浏览器、EJB 容器、.NET 应用程序、中间件基础结构和传统系统如何协调工作，从而确保企业 Web 服务系统的安全。

0.3　本书的读者对象

本书的读者对象是那些对使用 Web 服务的分布式企业计算系统的安全负责的人员。包括管理人员、架构师、编程人员和安全管理员。本书假设您具有将分布式计算系统应用于企业系统的经验，但是我们也不期望您具有大型分布式系统的安全经验。此外，XML、EJB 和.NET 方面的相关经验也很有用，但不是必需的。

应该注意的是，分布式安全不是一个简单的主题，所以读者不要期望仅仅通过阅读来吸收技术性很强的内容。另外，我们不希望本书的读者没有针对性地去学习本书的每个部分。

管理人员应该阅读第 1、2、3、12 章和其他章节的简介和小结部分。如果管理人员对某些章节有特殊的责任或兴趣，我们建议他们钻研相关章节。

我们建议架构师和编程人员应该阅读本书所有的章节，尽管编程人员可能只需要略读第 1 章和第 3 章。对于那些熟悉 ASP.NET 安全的读者来说，可以略读第 8 章，而那些熟悉 J2EE 的读者可以略读第 9 章。我们建议您即使对书中介绍的技术非常熟悉也要略读一下，因为书中一些信息非常新颖，在其他的地方可能接触不到。

安全管理员应该特别注意第 4、5、10、11 和 12 章。此外，他们还应该阅读第 3 章和第 7 章，而且至少还应该阅读其他章节的简介和小节。

0.4　资源 Web 站点

我们的资源 Web 站点网址是：www/wiley.com/compbooks/hartman，该站点上包含确保虚拟企业 ePortal 和 eBusiness 安全的全部源代码，这两个虚拟企业一直作为本书示例使用。Web 站点上还包含本书所有的勘误表和更新。

因为分布式安全是一种活跃的并不断发展的技术，因此我们将在书中不断地让您了解那些正在发展或淘汰的分布式安全技术，以及那些刚刚出现的分布式安全新技术。

0.5　小结

如果不想让自己的企业出现在晚间新闻中，标题是“据报道，<您企业的名称>被黑客非法侵入。这次侵入导致了重大财务损失，而且泄露了该公司大量客户的私人信息，其中包括被盗取的信用卡账户和密码”，您就应该很好地学习如何保护您的企业系统。这正是编写本书的初衷，本书将教您在部署 Web 服务时如何保护自己的企业。我们先从 Web 服务开始介绍各种安全技术和概念，然后再把 Web 服务接口与您的分布式系统的其余部分联系起来。

在企业安全中，一个脆弱的环节就可能导致整个企业安全的失败。因此，我们分别描述您公司各个部分的安全，从越过周边防火墙的客户、供应商和合作伙伴，到确保企业系统核心部分的安全。通过运用大量理论和示例，我们将指导您如何建立一个安全的 Web 服务系统，以及如何预测和筹备将来的安全系统。

在您部署和升级公司企业系统安全的时候，我们相信您能够把前面讨论的理论、概念和方法运用到分布式 Web 服务安全中。在您深入研究这个协同计算的新计算范例时，需要综合运用所有这些能帮助您克服困难的技能。我们希望本书有关 Web 服务安全的介绍，能够对您有所帮助。

目　　录