安全技术经典译丛

Web商务安全设计与开发宝典

——涵盖电子商务与移动商务

Web Commerce Security: Design and Development

[美] Hadi Nahari, Ronald L. Krutz 著

杨金梅 译

价值非凡的新商务领域安全力作

真实、可用的Web商务安全解决方案

商务安全系统架构师和开发人员的必备指南

清华大学出版社

安全技术经典译丛

Web 商务安全设计与开发宝典
——涵盖电子商务与移动商务

[美] Hadi Nahari
Ronald L. Krutz 著

杨金梅 译

清华大学出版社

EISBN：978-0-470-62446-3

图书在版编目(CIP)数据

Web 商务安全设计与开发宝典——涵盖电子商务与移动商务/ (美) 纳哈瑞(Nahari, H.) (美) 克鲁兹(Krutz, R.L.) 著；杨金梅　译. —北京：清华大学出版社，2012.9
(安全技术经典译丛)
书名原文：Web Commerce Security: Design and Development
ISBN 978-7-302-29378-1
Ⅰ. ①W…　Ⅱ. ①纳…　②克…　③杨…　Ⅲ. ①电子商务—安全技术　Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字(2012)第 158587 号

责任编辑：王　军　刘伟琴
装帧设计：牛艳敏
责任校对：邱晓玉
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：23　　**字　　数**：560 千字
版　　次：2012 年 9 月第 1 版　　**印　　次**：2012 年 9 月第1 次印刷
印　　数：1～5000
定　　价：59.00 元

产品编号：042660-01

作者简介

Hadi Nahari 是一位安全专业人士，有着 20 多年的软件开发经验，做了大量设计、体系结构、验证、概念验证和安全系统实施等方面的工作。他设计并实施了大规模的高端企业解决方案和资源受限的嵌入式系统，主要关注安全、加密、漏洞评估和威胁分析以及复杂系统设计。他经常在美国和国际安全大会上发表演讲，领导并参与了 Netscape Communications、Sun Microsystems、摩托罗拉、eBay 和 PayPal 等许多大型公司的各种安全项目。

Ronald L. Krutz 是一位资深信息系统安全顾问，有着 30 多年的从业经验，研究领域涉及分布式计算系统、计算机体系结构、实时系统、信息保证方法和信息安全培训。他拥有电子和计算机工程学士学位、硕士学位和博士学位。他在信息系统安全领域的著作非常畅销。Krutz 博士是信息系统安全认证专家(CISSP)和信息系统安全工程专家(ISSEP)。

他合作编写了 *CISSP Prep Guide* 一书，已由 John Wiley & Sons 出版。Wiley 还出版了几本他参与编写的书，其中包括 *Advanced CISSP Prep Guide*、*CISSP Prep Guide, Gold Edition*、*Security+Certification Guide*、*CISM Prep Guide*、*CISSP Prep Guide，2nd Edition: Mastering CISSP and ISSEP*、*Network Security Bible*、*CISSP and CAP Prep Guide，Platinum Edition: Mastering CISSP and CAP*、*Certified Ethical Hacker(CEH) Prep Guide*、*Certified Secure Software Lifecycle Prep Guide, and Cloud Security*。Krutz 还编写了一本 *Securing SCADA Systems* 和三本微型计算机系统设计、计算机接口和计算机体系结构等领域的教科书。Krutz 博士有 7 项数字系统方面的专利，至今已发表技术论文 40 余篇。

Krutz 博士是宾夕法尼亚州的注册专业工程师。

技术编辑简介

David A. Chapa 是一家名为 Enterprise Strategy Group(ESG)的研究和战略咨询公司的资深分析师。他有着 25 年以上的计算机行业从业经验，主要研究领域涉及数据保护、数据灾难恢复和业务恢复实践。他在许多大公司都担当高级技术职位，其中包括 Cheyenne Software、OpenVision、ADIC、Quantum 和 NetApp。他曾在各种各样的行业活动中作特色发言，主题涉及灾难恢复、合规以及磁盘、磁带和云在恢复和备份策略中的使用等。他是世界公认的备份和恢复专家。David 也是全球网络存储工业协会(Storage Networking Industry Association，SNIA)数据保护和容量优化(Data Protection and Capacity Optimization，DPCO)委员会的成员，该组织致力于促进存储市场在数据保护和容量优化技术领域的发展与成功。

致　谢

感谢所有直接或者间接帮助过我和帮助我编写本书的人。特别感谢 Carol Long 的全程支持和参与；感谢 Adaobi Obi Tulton、Nancy Rapoport 和 Nancy Carrasco 的追求卓越和高标准；感谢 John Wiley & Sons 团队的所有参与者。感谢本书的技术编辑 David A.Chapa 为本书提出了宝贵的反馈意见，是他的工作提升了本书的技术精准度。也感谢我的合著者 Ronald L. Krutz 博士，在编写本书的过程中他教会了我很多东西。

要感谢的人太多了，但是有一个人是不可缺少的，没有您的耐心、没有您的最富有创意的体贴、鼓励、安慰与支持，就不可能完成这本书，谢谢您，Eva！

——Hadi Nahari

首先感谢 Wiley 团队、技术编辑和我的合著者。此外，还要感谢我的妻子 Hilda，感谢她在我编写本书时给予的支持和鼓励。

——Ronald L. Krutz

序一

技术创新正改变着世界上消费者的购物和付费方式。电子商务正在迅速发展，线上和线下购物的传统区别日趋模糊。有 4 种发展趋势正改变着人们的购物方式：移动商务的兴起、社会媒体的影响、数字商品的增加和更方便快捷地本地购物的技术实现。渐渐地，无论在什么时间，无论在什么地方，我们都会找到我们想要的一切！

在这特别让人兴奋和活跃的全球商务环境中，本书的问世简直是一场及时雨。Web 商务安全是将来我们购物和付费的根本。Web 正变得越来越与我们的生活息息相关。在一个消费者在屏幕和设备之间无缝移动以进行购物、支付和连接的世界中，安全是多么至高无上！

在 eBay，我们成功的关键是在设计、管理和规模化我们的全球商务和支付平台时都确保把安全嵌入用户体验之中。当然，这应该是任何在当今有线、数字界打拼的公司所应该首要考虑的内容。

我们在 eBay 和 PayPal 的全球平台支持着将近 1.9 亿活跃账户和用户。在 eBay，买家和卖家每年在全球范围的商品交易总量达到 600 亿美元。2010 年，消费者通过我们的 eBay 移动应用程序交易的商品总量达到 20 亿美元。预计到 2011 年，这个数字会成倍增长到 40 亿美元。PayPal 每年处理世界上 920 多亿美元的支付总量。2010 年，PayPal 处理的移动支付总量为 7.5 亿美元。预计到 2011 年，这一数字也会翻一番。

在达到这样一个全球规模和全球总量的情况下，我们必须认真对待安全问题。全世界的企业家、商人和消费者每一天都离不开我们的安全平台。可扩展性和安全性不可或缺，数据保护和隐私至关重要，确保可靠性至高无上。要想使一个高度互动、一周 7 天一天 24 小时实时进行的全球贸易和支付体验在一个方便、快捷的环境下进行，我们必须应对所有这些复杂情况。

为了竞争和成长，企业必须深深理解并管理 Web 商务安全。Hadi Nahari 和 Ron Krutz 是这个领域的两位领军人物，感谢他们在本书中与我们分享他们的知识和洞察力。这是给我们大家的一个礼物，是任何想要在当今全球电子商务界打拼和成功的人的必读物。

eBay 公司总裁兼首席执行官 John Donahoe

序二

Internet 正在以惊人的速度改变着我们的生活。由于软件的持续创新，这个改变日新月异。在这个全球互联的新时代，新一代的人很难想象没有 Web 网络的日子会是什么样子。

无处不在的 Web 网络使我们以过去不敢想象的方式提供着服务。Web 网络的无所不能造就了最完美、最方便的商务、付费和收费平台。电子商务的增长规模相当惊人，PayPal 在 2010 年第四季度中，每秒钟交易 3380 美元，比前一年增长了 28%！

伴随这一增长而来的是消费者对于他们所接收到的服务的快捷性、可用性和安全性的预期也不断增长。对于任何负责任的公司而言，核心任务是提供可行、可靠和安全的用户体验。本书展示了如何创建这样一个系统。

在 PayPal，我们坚信，在这个高度一体化的世界里，无论消费者使用什么样的访问渠道，我们都必须提供同样的服务。不管它是个人计算机、移动电话、平板电脑、网络电视，还是任何其他消费者电子设备，我们都能保证 PayPal 用户享受无可挑剔的既便捷又安全的使用体验。我们交付解决方案和服务时的核心价值观是：相信我们的用户值得拥有一切！

2010 年，PayPal 的净付款总额，即总交易量，占全球电子商务的 18%。年总收入为 34 亿美元，其中跨境贸易大约占据总交易量的 25%。移动商务是另一个爆炸性增长的领域，截止到 2014 年，世界上的移动支付市场预计将达到 6330 亿美元。这是一个激动人心的时刻，我们已经对发展业务做好了充分的准备，用 PayPal 便捷、可用和安全的方式来支持电子商务和移动商务的发展。

我们服务于全球的消费者，使他们能够安全便捷地控制自己的钱。 我们提供可扩展、可靠和安全的基础设施供消费者和商户便捷安全地使用。在本书中，Hadi Nahari 和 Ron Krutz 这两位国际公认的电子商务和移动商务安全领域的专家将展示如何以正确的方式实现它。

PayPal 总裁 Scott Thompson

前　言

电子商务活动无处不在，无论我们是否意识到，我们每天都在从事这一活动。总体来讲消费者电子设备特别是移动电话已经成为我们生活不可或缺的一部分。因为设备功能变得越来越强大，相互连接越来越广泛，使用越来越便捷，因此也就能够更好、更快和更可靠地执行越来越多的任务。设备已经成为我们与数码世界沟通的守门人，它们俨然已成为我们享受数字生活不可或缺的手段。如果把刚才提到的两种趋势结合在一起，您将看到下一个即将到来的数字浪潮：与社交网络交互、从事电子商务活动(如银行业)、在线订货等等，所有这些都用到消费者电子设备。所有这些活动都有一个共同的重要元素：它们接触和使用同一个东西。换句话说，当今的数字安全取决于设备和它们与之交互的系统的安全。如果存在这样一个东西，那么就必须有可靠的机制来安全可靠地管理它。

从系统设计人员的角度讲，保证这样一个复杂系统的安全任务非常巨大。在这个生态系统中有许多不同的因素需要同步运作，但在最初设计时它们并不协同工作。而从终端用户的角度讲，需求却简单得多，那就是安全可靠地使用这个系统！本书将阐述向消费者提供这样一个安全系统的意义所在，我们将重点放在电子商务和它的各种各样的形式(如移动商务)上。

尽管各个领域都应用了基本的信息系统安全原则，但是电子商务安全却对信息安全专家提出了特殊的挑战。软件和硬件技术都以惊人的速度在发展，黑客和服务提供者有大量计算能力可供使用，其成本越来越低。比如，有了云计算，一个人可以以一小时一美元或更少的成本利用巨大的计算机资源。这种能力既可以用于有益的活动，也可能用于从事恶意活动，如破解存储在电子商务数据库中用于保护关键的个人和金融交易信息的密钥。同样，今天在许多国家，手机可以提供用于免提扫描交易的信用卡功能。移动设备中的 RFID 读取能力在为各种各样的电子商务范式打开了大门之外，还为新的攻击方法打开了大门。因此，了解信息系统安全的电子商务方法对认识安全威胁和与此相关的对策是非常有必要的。

本书从整体和微观的角度解释了分析和理解系统安全的必要步骤，定义了风险驱动的安全、保护机制和如何最好地部署这些机制，提出了以一种可用的和对用户友好的方式来实施安全的方式方法。所有主题都是电子商务，但它们也适用于移动商务。下面列出了本书中涵盖的一些重要主题：

- 安全虽然防弹，但却难以使用，所以用户不愿意采用它。因此，设计和实施强大的、但对用户也友好的安全性非常重要。
- 如何使电子商务和移动商务更安全；如何设计和实施它。
- 实施适合的、风险驱动的和可扩展的安全基础设施的技巧。
- 架构高可用性和大交易容量的电子商务和移动商务安全基础设施的基础知识。
- 如何识别大规模交易系统中的弱安全性。

本书向系统架构师或者开发人员提供了设计和实施满足消费者需求的安全电子商务或移动商务解决方案所需的信息。如果读者还能了解到安全技术、漏洞评估和威胁分析、交易式和可扩展系统的设计、开发、维护以及支付和商务系统，那就是锦上添花了。

本书的组织结构

本书共有 9 章内容和 4 个附录，各章依次讲述了重要的背景信息和关于移动商务和移动商务安全问题的详细知识。附录提供了支撑各章节内容的重要的技术和合规主题。

本书一开始介绍了电子商务时代及它对消费者购买习惯所带来的影响。随后的几章重点介绍健壮而安全的电子商务系统所必须具备的重要特性，接下来介绍电子商务的基本构件块。有了这些信息作为基础，中间几章详细讨论了实施一个健壮的电子商务环境可以使用哪些工具和保护这样的环境需要用到哪些方法。最后的几章探讨验证电子商务实施的保证态势的方式方法。

第 1 章回顾分布式计算的基本概念，解释电子商务区别于传统商务的独特特点。也提到了数字商品、硬商品和支付方法，介绍了移动商务。

第 2 章讨论了消费者电子设备，深入研究了电子商务和移动商务的不同之处。然后继续详细地讨论移动硬件、操作系统和栈。该章也探讨了瘦客户端和厚客户端、应用程序仓库和不同的移动 carrier 网络的特点。

第 3 章讨论了电子商务系统中的一些重要特性，如可用性、互操作性、可靠性和可扩展性等等。

有了前面几章作基础，第 4 章关注电子商务安全，包括构成电子商务系统安全的要素、风险管理以及计算机系统的可扩展性和相应的安全措施。结尾部分提供了如何保证电子商务交易安全的宝贵资料。

第 5 章讨论各种各样的电子商务保护措施，包括密码学、访问控制类型和机制、系统硬化和 Web 服务器安全。该章还进一步探讨了适用于电子商务系统的主机级和网络级安全措施。

第 6 章描述了支撑安全可靠交易所必须用到的关键电子商务系统安全组件和原则。其中包括验证类型、授权、隐私、数据分级以及系统与数据审计。然后，该章还探讨了纵深防御、最小特权、信任和通信安全等原则。

为了实施恰当的安全控制措施，了解电子商务实施中现存的漏洞非常重要。第 7 章涉及漏洞评估、入侵检测和防御、扫描工具、搜索软件和渗透测试。

第 8 章讨论了电子商务系统面临的威胁，涉及 Web 应用程序、攻击树、滥发、钓鱼、

数据采集、跨站脚本、Web 服务攻击、rootkit 和各种各样其他的关键威胁主题。

第 9 章是最后一章，提到了认证问题，比如评价类型、标准、保证、文档和认证类型，如 MasterCard CAST、通用标准、GlobalPlatform Card Composition Model 等等。

附录 A 概述了电子商务历史和基本的电子商务概念，讨论了硬件、软件和虚拟化问题以及安全隔离的重要性。也探讨了电子商务系统中的操作系统、网络、存储和中间件等主题。

附录 B 提供了有关电子商务标准化和管理机构的相关信息。

附录 C 是重要术语表。

附录 D 是本书所用到和推荐阅读的一些参考文献。

读者对象

本书的主要读者应该是架构师和开发人员、系统工程师、项目经理、高级技术经理、公司战略人士和技术营销人员。

本书的理想读者应该是从技术上需要了解如何设计和实施满足消费者需求的安全电子商务或移动商务解决方案的系统架构师或开发人员。这样的读者应该具备了安全技术、漏洞评估和威胁分析、交易式和可扩展系统的设计、开发、维护以及支付和商业系统等方面的知识，不需要什么特殊工具。

小结

Internet、Web 和电子商务对我们的日常生活所造成的深刻影响无须再提。个人计算机、移动电话和其他消费者电子设备成为了我们与数码世界交互的守门人，它们俨然已成为我们享受数字生活的不可或缺的手段。因为我们使用移动设备进行商务交易，所以电子商务使我们对 Web 的依赖越来越大。浏览电子商务网站的首页(比如，当您浏览 www.ebay.com 时看到的第一页)并登录您的账户似乎是一个非常简单的动作，但是，使这一过程安全可靠却不是那么简单的事。

数字安全几乎完全依赖于计算机、移动设备和它们所连接的所有系统的安全，这是一个非常复杂的设置。我们都需要可靠的安全，因此实施安全进程以满足这一需要并保护我们的机密信息至关重要。从系统设计人员的角度讲，保证这样一个复杂系统的安全任务非常巨大。在这个生态系统中有许多不同的部分需要同步运作，但在最初设计时它们并不协同工作。而从终端用户的角度讲，需求却简单得多，那就是便捷、安全和可靠地使用这个系统!本书将阐述构建安全的电子商务和移动商务系统从而供消费者放心使用的意义所在!

目　录

第Ⅰ部分

商 务 概 览