<<Web商务安全设计与开发宝典>>

图书基本信息

书名：<<Web商务安全设计与开发宝典>>

13位ISBN编号：9787302293781

10位ISBN编号：7302293783

出版时间：2012-9

出版时间：清华大学出版社

作者：(美) 纳哈瑞(Nahari, H.),(美) 克鲁兹(Krutz, R.L.)

页数：346

字数：560000

译者：杨金梅

<<Web商务安全设计与开发宝典>>

内容概要

每个系统设计人员都知道，保护电子商务生态系统的安全简直就是噩梦一每当我们使用计算机网络进行银行交易、账单支付、购物或者在线交流时，我们重要的企业信息和个人信息便置于风险之中二

在《Web商务安全设计与开发宝典：涵盖电子商务与移动商务》中，安全专家Hadi Nahari和Ronald
L.Krutz提供了真实的安全解决方案。
他们从宏观和微观的角度展示了如何分析和理解这些解决方案，定义了风险驱动的安全，解释了什么是保护机制和怎样才能最好地部署这些机制，提供了既有效又对用户友好的安全实施方式。

《Web商务安全设计与开发宝典：涵盖电子商务与移动商务》主要内容
●设计强大的、用户会真正使用的电子商务和移动商务安全
●实施自适应的、风险驱动的和可扩展的安全基础设施
●构建具有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
●理解解决方案必须具备的各个重要特性
●识别大规模交易系统中的弱安全以及如何增强安全性
●了解具体的漏洞和威胁以及如何评估、检测和预防它们

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。

Hadi Nahari是eBay和PayPal公司的主要安全架构师和移动架构师他有着大规模的高端企业解决方案和嵌入式系统方面的丰富经验，主要关注安全、密码学、复杂系统设计、漏洞评估和威胁分析他是安全问题方面最受欢迎的发言人。

RonaldL.Krutz博士是卡耐基·梅隆研究院网络安全中心的创始人他有着计算机架构、实时系统和信息安全等领域40多年的从业经验，曾主编或参编了大量书籍。

Ronald.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 -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。

书籍目录

章节摘录

版权页： 插图： 安全并非静态的。
这也就是说，您不能认为放置一套显著的认证机制和一个有效的授权子系统并实施分层安全之后就万事大吉了，系统就永远安全了。
事实远不止于此。
首先，我们基本不可能穷尽所有针对电子商务系统的攻击，因此也就不可能阻止或者防卫这些攻击。
此外，成为安全资产的这个对象的所有特点有可能随着时间的推移而变化，和其他对象或者安全资产的关系也发生变化。
比如，以您的电子邮件地址为例。
电子邮件地址本身可能并不是一个有价值的东西，因为从概念上讲它只是一个公共信息（否则其他人将不能给您发信息）。
但是，如果电子商务系统用您的电子邮件地址和您当前的位置、您计算机的IP地址或者可能是您的浏览器中的一个cookie（所有这些都有可能被攻击者通过可搜索到的社会媒体内容和简单的cookie劫持攻击而获取）来识别您的话，那么这个电子邮件地址便成为一个安全资产。
也就是说，判断一个资产是否是安全资产，进而判断是否提供有效的保护机制来保护它，是根据情况而定的。
您与Internet互动的越多，您越积极主动，识别安全资产并设计安全机制的工作就会变得越复杂。
这使得安全专家的工作成为一个复杂、动态和敏感的艺术工作，正如安全领域本身那样。
这种复杂性不仅体现在设计和实施阶段，而且渗透到电子商务系统的操作和维护方面。
4.3 风险驱动安全 风险驱动安全是一种先进理念。
电子商务系统的一个主要支柱是从操作、交易和财务的角度和整个功能的方方面面进行风险管理。
为了更好地理解风险驱动安全，首先必须理解风险是什么。
风险是一个事件在未来可能发生或被避免或被减轻的数学概率，而不是当下能够造成伤害而必须立即解决的现有问题。
这听起来有些绕口。
用外行人的话讲，风险是某些事件发生的概率，而并非指它实际出现。
另一方面，风险驱动安全是指设计和实施安全措施的理念，这些安全措施的部署基于攻击出现的概率。
这与静态安全设计理念大有不同，后者直接处理诸如电子商务基础设施这样的可扩展的系统的安全优化问题。
让我们看看这是什么意思。

编辑推荐

《Web商务安全设计与开发宝典:涵盖电子商务与移动商务》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。

版权说明