<<电子商务安全>>

图书基本信息

书名：<<电子商务安全>>

13位ISBN编号：9787303117697

10位ISBN编号：7303117695

出版时间：2011-1

出版时间：北京师范大学出版社

作者：李洪心 编

页数：372

<<电子商务安全>>

内容概要

本书共14章，分三大部分。
第一部分是理论基础，从第一章到第四章，介绍了电子商务面临的安全问题和电子商务安全技术基础，具体包括电子商务安全概述、加密技术、数字签名与消息认证技术、公钥基础设施PKI。
电子商务安全可以分为信息传输与访问过程中的安全，以及电子商务系统的安全，第二部分和第三部分分别介绍实现这两方面的相关技术。
第二部分从第五章到第八章，介绍了电子商务安全协议(重点介绍SSI．协议和SE丁协议)、网上支付安全、移动商务安全、移动支付安全、电子商务身份认证和电子商务访问控制。
第三部分从第九章到第十四章，重点介绍了计算机及其网络的安全，以及电子商务系统的安全，内容包括防火墙与虚拟专用网、网络攻击、计算机病毒、入侵检测系统与应急处理、电子商务系统的容错以及电子商务系统的审核与取证。
为了方便不同知识背景电子商务专业的教师和学生使用本书，作者在书中用+号注明了有一定难度和开放性的选学内容。

<<电子商务安全>>

书籍目录

章节摘录

版权页：插图：传统上，公司一般采用防火墙作为安全的第一道防线。
而随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙策略已经无法满足对安全高度敏感的部门的需要，网络的防卫必须采用一种纵深的、多样的手段。
与此同时，当今的网络环境也变得越来越复杂，各式各样复杂的设备需要不断升级，存在漏洞的系统使得网络管理员的工作不断加重，不经意的疏忽便有可能造成重大的安全隐患。
在这种环境下，入侵检测系统成为安全市场上新的热点，不仅越来越多的受到人们的关注，而且已经开始在各种不同的环境中发挥其关键作用。
入侵检测（Intrusion Detection）是对入侵行为的检测。
它通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。
入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵，因此被认为是防火墙之后的第二道安全闸门，能在不影响网络性的情况下能对网络进行监测，是防火墙的合理补充。
从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视。
入侵检测主要有以下几个方面的功能：（1）网络访问控制。
入侵检测使用基本规则定义可以访问特定网络资源的用户，从而确保只对网络资源进行授权访问。
（2）高级反病毒引擎。
能够探测包含计算机病毒的网络流量的病毒扫描引擎，它可以防止用户在不知情的情况下下载受病毒感染的文件。
（3）全面的攻击模式库。
入侵检测可以自动探测来自网络流量的攻击模式。
定期更新的攻击模式库可以能够确保入侵检测保持最新。
（4）包检测技术。
入侵检测在隐蔽模式下工作，攻击者是察觉不到的。
由于黑客不知道他们正在被监视，攻击通常在黑客未察觉的情况下被捕获。
（5）URL阻塞。
管理员可以指定不允许用户访问的URL，从而防止了非工作性web冲浪。
（6）内容扫描。
管理员通过入侵检测可以定义策略对内容进行检查。
这可以防止在没有授权的情况下通过电子邮件或web发送敏感数据。
（7）网络使用情况记录。
入侵检测允许网络管理员跟踪最终用户、应用程序等的网络使用情况。
它有助于改进网络策略规划和提供精确的网络收费。

编辑推荐

《电子商务安全》是新世纪高等学校教材,电子商务核心课系列教材之一。

版权说明