<<计算机网络安全导论>>

图书基本信息

书名：<<计算机网络安全导论>>

13位ISBN编号：9787121087035

10位ISBN编号：7121087030

出版时间：2009-5

出版时间：电子工业出版社

作者：（美）奥巴代特，（突尼斯）布德里卡 著，毕红军，张凯 译

页数：260

前言

计算机网络安全无疑算得上是当今计算机学界的“显学”，一时研究者云集，成果迭出，各高校也都纷纷开出网络安全的课程或专业。
然而，由于计算机网络安全涉及领域太广，初学者往往不知从何下手，即便是本领域的从业者，也时有“只缘身在此山中”的茫然。
究其原因，主要是目前的网络安全教材和图书中，专注于某一问题、某一技术、某一产品的比较多，而具备全局视点，能够综合梳理整个领域，进而拼接出网络安全的全景视图的则少得多。
本书正是这样一种努力的成果，试图从原理到技术、从框架到应用、从软硬件系统到管理规程制度，自底向上，逐层剖析，以求尽可能全面地介绍电子系统与计算机网络安全的各个核心领域。
可以说，本书最显著的特点之一，就是内容全面，这体现在如下几个方面：一是介绍的面比较广，举凡公钥密码体制、数字签名技术、PKI、生物测量技术、电子信任管理、电子服务、电子商务、电子政务、WLAN、IDS、VPN、恶意软件防护、风险管理等无所不包，而且详略得当，重点突出；二是对于重要的问题，不仅仅满足于泛泛介绍，而且阐明其理论基础，并往往给出示例，便于理解；三是对于各类安全技术，不仅介绍其原理和功能，而且也专门讨论其面临的挑战与问题，例如，关于RSA算法，除了介绍其概念、原理和示例，还专门用一节的篇幅介绍针对RSA的攻击技术的发展。
本书的第二个显著特点，就是观点新颖。
这体现在：一方面，本书介绍了许多新技术和近年来的热点问题，例如生物测量技术、SOA、移动商务、移动政务、WI。
．AN安全等；另一方面，书中引入的大量参考资料，大多数是近年来比较有权威性的著作，其所引用的统计图表和产品列表，都是比较晚近的数据，例如，第1章引用的调查报告，是最近两三年的数据，而第13章讨论的各种防护软件，大部分现在还在销售；此外，书中还提出了作者自己的新的研究成果，例如生物测量中的击键节奏测量技术、风险分析中的NetRAM框架等。
本书的第三个显著特点，就是贴近实际。
本书不仅介绍了近年来学界的研究成果，而且总结了业界的实践经验，甚至还分析了当前市场上的相关产品。
众所周知，网络安全绝不仅仅是个技术问题，而是“三分技术、七分管理”，为此，本书用了不少篇幅从企业安全经理（或CSO）的角度出发，分析了网络安全所涉及的项目规划、风险分析、文档准备、制度制定等管理要素，寓理论于实践，对网络安全从业人员有着较强的指导作用。

<<计算机网络安全导论>>

内容概要

本书系统地介绍了计算机网络安全各个核心领域，自底向上，逐层剖析，从安全服务基础、公钥密码体制和数字签名技术入手，描述了PKI、生物测量和电子信任等各种安全工具与技术框架，讨论了电子服务、电子政务、电子商务和WLAN安全等应用，并且重点研究了包括IDS、VPN、恶软防护和风险管理在内的企业级防护手段与技术。
本书有三个突出特点：一是内容全面，全面梳理了整个网络安全领域的研究现状，内容广博、视野开阔，提供了该领域的全景视图：二是观点新颖，体现了近年来网络安全领域的最新成果；三是贴近实际，以企业级安全防护为着眼点，统合学界成果和业界实践。
本书对计算机、电信、信息学、系统与软件工程等专业的科研人员和网络安全从业人员来说，是一本不可多得的参考书，并且也十分适用于用做研究生或高年级本科生的网络安全、信息系统安全、通信系统安全、电子系统安全等课程的教科书。

作者简介

作者：(美国)Mohammad S.Obaidat (突尼斯)Noureddine A.Boudriga 译者：毕红军 张凯Mohammad S.Obaidat，美国新泽西州蒙茅斯大学计算机科学专业教授，因其在网络与信息安全等领域的开创性、持续性贡献而闻名于世。
他勤于笔耕，著述颇丰。
他在俄亥俄州立大学获得博士学位，并获多项奖项。
他现在是SCSI和IEEE的研究员。
Noureddine A．Boudriga，在法国巴黎第11大学获得数学博士学位，在突尼斯的突尼斯第2大学获得计算机科学博士学位，现任突尼斯迦太基的11月7日大学通信工程学院电信专业教授，并担任网络与安全研究实验室主任。

<<计算机网络安全导论>>

书籍目录

章节摘录

插图：第1部分电子安全简介在企业级系统中，安全暴露（Exposure）是指可能对企业的信息和通信系统造成损害的情形，例如，未授权的信息泄露、篡改业务及员工数据、拒绝对信息系统的合法访问等，而漏洞（Vulnerability）则是指系统中那些可能被对手利用并造成损失和危害的系统薄弱环节。
入侵者指的是那些利用系统漏洞，对信息或生产系统实施安全攻击的对手。
当前，电子安全对企业和政府而言都是一个重要问题。
电子安全旨在加强公司的安全，找到系统漏洞，并监督公司在线服务保护机制的运行情况，以便N-ak对手（如黑客、恶意用户、入侵者等）进入公司的网络、计算机和服务。
电子服务与电子隐私的概念有着密切的联系，有时甚至难分彼此。
电子隐私问题可以导致用户或业务被追踪，了解他们访问企业网站时的所作所为。
不论公司业务规模是大是小，也不论公司网络是开放式还是封闭式的，任何公司都应当把确保公司业务安全作为重中之重。
为此，公司内部应当建立起一套安全策略，以涵盖密码使用规则、访问控制、数据安全机制和商业交易（Transaction）保护等问题。
任何公司都应当遵循的一套好的行为准则包括：（a）持续更新病毒扫描软件和病毒响应工具；（b）对敏感数据可以考虑使用独立的计算机（即不联网的计算机）；（c）根据业务活动的组织形式来定义适当的可信域；（d）根据安全策略安装恶意行为监测系统；（e）对电子邮件管理制定严格规范（特别是对那些来自未知源地址并带有已知扩展名附件的电子邮件）。
电子安全方案旨在提供5种重要服务，即用户鉴别、系统完整性、通信保保密性、业务服务可用性和交易抗抵赖性。
本书中提供的大多数电子安全方案都使用了两种主要的密码技术：公钥密码体制和数字签名。
有效的解决方案还必须符合国家相关法律的规范。
本书的第1部分旨在定义电子安全中的常用概念，也讨论了公司安全系统中的主要技术和挑战。
本问分对安全攻击和安全服务做了分类，并讨论了其主要的问题。
本部分包含3章：第1章 阐述了系统安全的重要性，并提出了网络安全和用户防护方面的相关概念。
本章还介绍了全书中用于定义服务、信息、计算机安全和网络安全的一些基本术语。
本章旨在使本书所述内容能够自成体系。
第2章 讨论了加密及其实际应用，主要关注公钥密码体制中使用的几种技术。
本章也详细介绍了密码的不同种类，及其在提供基础电子服务方案中的应用。
本章向读者提供了一些简单的例子，以解释那些主要概念和手段是如何行之有效的。

编辑推荐

《计算机网络安全导论》由电子工业出版社出版。
当今世界，电子系统与计算机网络无处不在，其应用面涵盖电子商务、无线局域网（WLAN）、医疗部门、政府机关等。
因此，信息的安全传输就成为研究、开发和投资的重要领域。
《计算机网络安全导论》介绍了电子系统与计算机网络安全的基本概念、工具和协议，及其广泛的应用。
《计算机网络安全导论》详细介绍了电子系统与计算机网络安全的核心领域，例如用户鉴别、系统完整性、通信保密性、业务服务可用性、交易抗抵赖等。
同时介绍了电子安全的主要趋势、挑战和应用，特别强调了公钥基础设施（PKI）体系、基于生物测量的安全系统、信任管理系统、电子服务范式。
书中还讨论了入侵检测系统、虚拟专用网（VPN）、恶意软件、WLAN安全和风险管理，此外，《计算机网络安全导论》对电子商务、电子政务、电子服务等应用领域都有所涉及。
《计算机网络安全导论》可作为高年级本科生或研究生的计算机网络安全、信息系统安全、通信系统安全、电子系统安全等课程的教科书。
由于《计算机网络安全导论》又着眼技术、实例丰富，对网络与信息安全领域从业人员来说，也是一本不可多得的参考书。

版权说明