<<计算机安全>>

图书基本信息

书名：<<计算机安全>>

13位ISBN编号：9787111292470

10位ISBN编号：7111292472

出版时间：2010-1

出版时间：机械工业出版社

作者：斯托林斯，布朗 等著

页数：798

前言

BACKGROUND Interest in education in computer security and related topics has been growing at a dramatic rate in recent years. This interest has been spurred by a number of factors, two of which stand out: 1. As information systems, databases, and Internet-based distributed systems and communication have become pervasive in the commercial world, coupled with the increased intensity and sophistication of security-related attacks, organizations now recognize the need for a comprehensive security strategy. This strategy encompasses the use of specialized hardware and software and trained personnel to meet that need. 2. Computer security education, often termed information security education or information assurance education has emerged as a national goal in the United States and other countries, with national defense and homeland security implications Organizations such as the Colloquium for Information System Security Education and the National Security Agency's (NSA's) Information Assurance Courseware Evaluation (IACE) Program are spearheading a government role in the development of standards for computer security education. Accordingly, the number of courses in universities, community colleges, and other institutions in computer security and related areas is growing. OBJECTIVES The objective of this book is to provide an up-to-date survey of developments in computer security. Central problems that confront security designers and security administrators indude defining the threats to computer and network systems, evaluating the relative risks of these threats, and developing cost-effective and user-friendly countermeasures. The following basic themes unify the discussion: Pfindples: Although the scope of this book is broad, there are a number of basic principles that appear repeatedly as themes and that unify this field. Examples are issues relating to authentication and access control. The book highlights these principles and examines their application in specific areas of computer security. Design approaches: The book examines alterna,tive approaches to meeting specific computer security requirements Standards: Standards have come to assume an increasingly important, indeed dominant, role in this field. An understanding of the current status and future direction of technology requires a comprehensive discussion of the related standards. Real-world examples: A number of the chapters include a section that shows the practical application of that chapter's principles in a real-world environment. INTENDED AUDIENCE The book is intended for both an academic and a professional audience. As a textbook, it is intended as a one- or two-semester undergraduate course for computer science, computer engineering, and electrical engineering majors, It covers all the topics in 0S7 Security and Protection, which is one of the core subject areas in the IEEE/ACM Computer Curricula 2001,as well as a number of other topis The book covers the core area lAS Information Assurance and Security in the Computer Curricula 2005 Information Technology Volume; and CE-OPS6 Security and Protection from the Computer Engineering Curriculum Guidelines, 2004. For the professional interested in this field, the book serves as a basic reference volume and is suitable for self-study. PLAN OF THE TEXT The book is divided into six parts (see Chapter 0): · Computer Security Technology and Principles · Software Security · Management Issues . · Cryptographic Algorithms · Internet Security · Operating System Security The section on OS security covers two real-world examples in detail: Linux and Windows Vista. There are also a number of appendices in the book to provide additional background.The book is also accompanied by a number of online appendices that provide more detail on selected topics The book includes an extensive glossary, a list of frequently used acronyms, and a bibliography. Each chapter includes homework problems, review questions, a list of key words,suggestions for further reading, and recommended Web sites. HACKING EXERCISES The instructor's support materials include two Web related hacking exercises: (1) Cross site scripting attacks (2) Server side SQL injection type attacks For both of the above the instructor needs a Linux system with a web server installed (Apache is freely available and could work as a web server) as well as PhP installed (again, its freely available). You simply download the files from the instructor support site and save them in the public html directory, and unpack them for the projects to be ready to use. You would of course also need to change the permissions on the folders and the files after you unpack it but that's easy. Also included is a short step-by-step instruction manual that tells the instructor exactly what to do with this package of files in order to create the environment for the student exercises. These projects have been used in computer security courses and

have been the highlight of the courses; students felt the most excited because of them and they are very rewarding indeed. An additional hacking exercise is included that involves attempting to reverse engineer an application-level protocol. This is a sockets programming exercise. See Appendix C in this book for more details. OTHER PROJECTS AND STUDENT EXERCISES For many instructors, an important component of a computer security course is a project or set of projects by which the student gets hands-on experience to reinforce concepts from the text. Tnis book provides an unparalleled degree of support for including a projects component in the course. The instructor's supplement not only includes guidance on how to assign and structure the projects but also includes a set of user's manuals for various project types plus specific assignments, all written especially for this book. Instructors can assign work in the following areas: · Programming projects: A series of programming projects that cover a broad range of topics and that can be implemented in any suitable language on any platform · Research projects: A series of research assignments that instruct the student to research a particular topic on the Intemet and write a report · Laboratory exercises: A series of projects that involve programming and experimenting with concepts from the book · Practical security assessments: A set of exercises to examine current infrastructure and practices of an existing organization · Reading/report assignments: A list of papers that can be assigned for reading and writing a report, plus suggested assignment wording · Writing assignments: A list of writing assignments to facilitate learning the material This diverse set of projects and other student exercises enables the instructor to use the book as one component in a rich and varied learning experience and to tailor a course plan to meet the specific needs of the instructor and students, See Appendix C in this book for details. INSTRUCTIONAL SUPPORT MATERIALS To support instructors, the following materials are provided: · Solutions Manual: Solutions to end-of-chapter Review Questions and Problems · PowerPoint slides: A set of slides covering all chapters, suitable for use in lecturing. · PDF files: Reproductions of all figures and tables from the book · Projects manual: Suggested project assignments for all of the project categories listed below Instructors may contact their Pearson Education or Prentice Hall representative for access to these materials In addition, the book's Web site supports instructors with · Links to Webs sites for other courses being taught using this book · Sign-up information for an Internet mailing list for instructors INTERNET SERVICES FOR INSTRUCTORS AND STUDENTS There is a Web site for this book that provides support for students and instructors. The site includes links to other relevant sites. The Web page is at WilliamStalling&com/CompSec/CompSecle.html; see Chapter 0 for more information. An Intemet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and with the author. As soon as typos or other errors are discovered, an errata list for this book will be available at WilliamStalhngs. com. ACKNOWLEDGMENTS This book has benefited from review by a number of people, who gave generously of their time and expertise. The following professors and instructors reviewed all or a large part of the manuscript: James Bret Michael (Naval Postgraduate School), Scott Campbell (Miami University), Jim Aires-Foss (University of Idaho), Gregory B. White (University of Texas-San Antonio), Corey D. Shou (Idaho State University), Weining Zhang (University of Texas——San Antonio), Sreekanth Malladi (Dakota State University), Breno Fonseca De Medeiros (Florida State University), Kent E. Seamons (Brigham Young University),Krishna M. Sivalingam (University of Maryland, Baltimore County), and Alec Yasinsac (Florida State University). Thanks also to the many people who provided detailed technical reviews of one or more chapters: Pradeep Navalkar (TechTonics Group Limited); Manish Gupta (M&T Bank Corporation, Buffalo); Scott W. DeVault (CISSP, MCP, The AEgis Technologies Group, Inc.); Arturo 'Buanzo' Busleiman (Independent Security Consultant, Buenos Aires); David Grant (MICDDS, Group Security Manager, Halcrow Group Ltd); Spike Ouatrone; Jaspreet Singh (Senior Consultant, Ernst and Young, India): Jean-Charles Demarque (IT Consultant in France); Steve Fletcher; David Oillett (CISSP, CCNP, CCSE,MCSE); Robert Slade (author and prolific book reviewer); Rob J. Meijer (Dutch National Police Agency); Marc Blitz (aacompsec.com); Kevin Sanchez-Cherry (IT security and assurance specialist); Don Munro; Edward Lewis (Australian Defence Force Academy, University of New South Wales); and Jerome Athias (Independant Security Researcher). Sreekanth Malladi of Dakota State University developed the Web hacking projects.Arnold Patton of Bradley University developed the reverse engineering hacking project. We also thank Ricky Magalhaes of Fastennet

Security, who developed a series of Windows security projects for this book. The following people provided homework problems: Zubair Baig (Monash University);Spike Quatrone; Edward Lewis (University of New South Wales), and Rob J Meijer. Dr Lawrie Brown would first like to thank Bill Stallings for the pleasure of working with him to produce this text. I would also like to thank my colleagues in the School of Information Technology and Electrical Engineering, University of New South Wales at the Australian Defence Force Academy in Canberra, Australia for their encouragement and support.I particularly wish to acknowledge the insightful comments and critiques by Ed Lewis and Don Munro, who I believe have helped produce a more accurate and succinct text. Finally, we would like to thank the many people responsible for the publication of the book, all of whom did their usual excellent job. This includes the staff at Prentice Hall, particularly my editor, Tracy Dunkelberger, her assistants, Christianna Lee and Carole Snyder, and production manager, Rose Kernan. Thanks also to Patricia M. Daly, who did the copy editing.

<<计算机安全>>

内容概要

本书系统地介绍了计算机安全领域中的各个方面，全面分析了计算机安全威胁、检测与防范安全攻击的技术方法以及软件安全问题和管理问题。
本书重点介绍核心原理，揭示了这些原理是如何将计算机安全领域统一成一体的，并说明了它们在实际系统和网络中的应用。
此外，本书还探讨了满足安全需求的各种设计方法，阐释了对于当前安全解决方案至关重要的标准。
本书思路清晰，结构严谨，并且提供了扩展的教学支持——数百个精心设计的实践问题，是高等院校计算机安全专业的理想教材，同时也可作为研究人员和专业技术人员的非常有价值的参考书。

作者简介

William Stallings拥有美国麻省理工学院计算机科学博士学位，现任教于澳大利亚新南威尔士大学国防学院（堪培拉）信息技术与电子工程系。
他是世界知名计算机学者和畅销教材作者，已经撰写了17部著作，出版了40多本书籍。
内容涉及计算机安全、计算机网络和计算机体系结构等方面

<<计算机安全>>

书籍目录

章节摘录

插图：The subsection on threats to communication lines and networks in Section 1.2 is based on the X.800 categorization of security threats.The next two sections exam ine security services and mechanisms, using the X.800 architecture.Security Services X.800 defines a security service as a service that is provided by a protocol layer of ommunicating open systems and that ensures adequate security of the systems or of data transfers Perhaps a clearer definition is found in RFC 2828, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.X.800 divides these services into six categories and fourteen specific services (Table 1.5). We look at each category in turn.5 Keep in mind that to a considerable extent, X.800 is focused on distributed and networked systems and so emphasizes network security over single-system computer security. Nevertheless, Table 1.5 is a useful checklist of security services.Authentication The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic; that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can asquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.Two specific authentication services are defined in the standard:Peer entity authentication: Provides for the orroboration of the identity of a peer entity in an association. Two entities are considered peer if they imple ment the same protocol in different systems (e.g., two TCP users in two com municating systems). Peer entity uthentication is provided for use at the establishment of, or at times during the data transfer phase of, a onnection. It attempts to provide confidence that an entity is not performing either a mas querade or an nauthorized replay of a previous connection.Data origin authenticatio: Provides for the corroboration of the source of a data unit. It does not provide otection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.Access Control In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must irst be identified, or authenticated, so that access rights can be tailored to the individual.There is no universal agreement about many of the terms used in the security literature. For example, the term integrity is sometimes used to refer to all aspects of information security. The term authentication is sometimes used to refer both to verification of identity and to the various functions listed under integrity in the this hapter. Our usage here agrees with both X.800 and RFC 2828.

编辑推荐

《计算机安全原理与实践(英文版)》是由机械工业出版社出版的。

版权说明