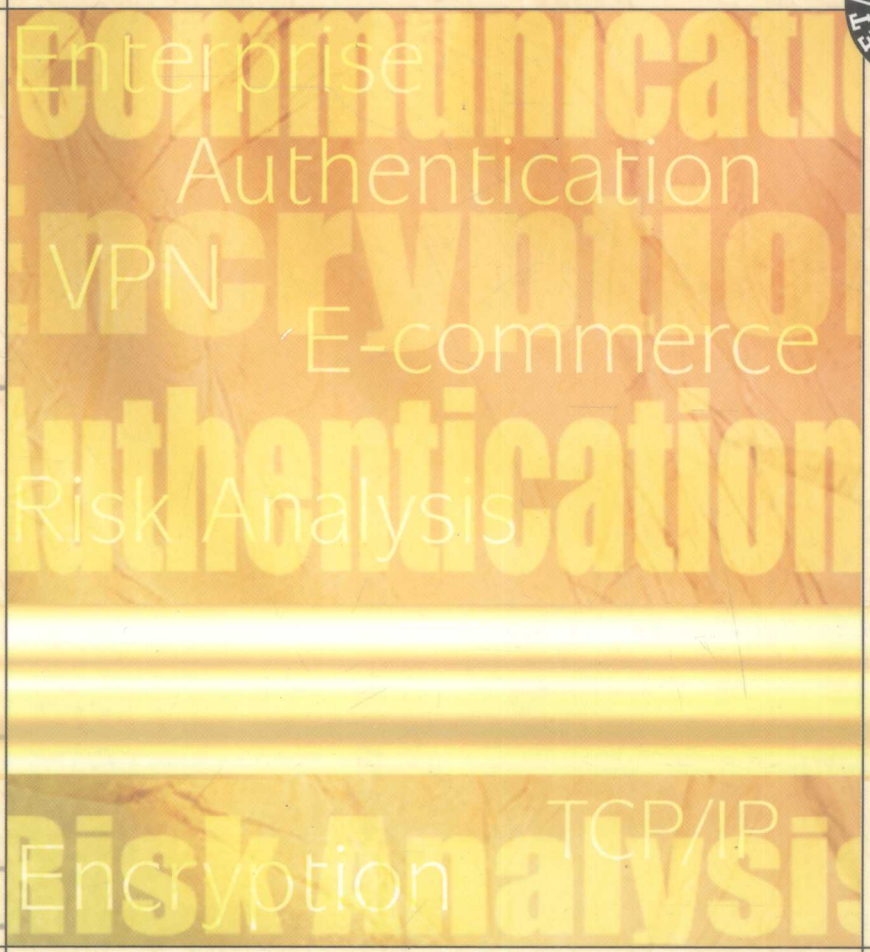
THOMSON
DELMAR LEARNING

Network Security



Pardoe
& Snyder

NETWORK SECURITY

Terry D. Pardoe
Gordon F. Snyder, Jr.

THOMSON
DELMAR LEARNING
Australia Canada Mexico Singapore Spain United Kingdom United States

THOMSON
DELMAR LEARNING

Network Security

by Terry D. Pardoe and Gordon F. Snyder, Jr.

Vice President, Technology and Trades SBU:
Alar Elken

Editorial Director:
Sandy Clark

Senior Acquisitions Editor:
Steve Helba

Senior Development Editor:
Michelle Ruelos Cannistraci

Marketing Director:
Dave Garza

Channel Manager:
Fair Huntoon

Marketing Coordinator:
Casey Bruno

Production Director:
Mary Ellen Black

Production Manager:
Larry Main

Production Editor:
Dawn Jacobson

Senior Project Editor:
Christopher Chien

Art/Design Coordinator:
Francis Hogan

Technology Project Manager:
Kevin Smith

Technology Project Specialist:
Linda Verde

Senior Editorial Assistant:
Dawn Daugherty

Printed in the United States of America
1 2 3 4 5 XX 07 06 05

For more information contact
Thomson Delmar Learning
Executive Woods
5 Maxwell Drive, PO Box 8007,
Clifton Park, NY 12065-8007
Or find us on the World Wide Web at
http://www.delmarlearning.com

For permission to use material from this text or product, contact us by
Tel. (800) 730-2214
Fax (800) 730-2215
http://www.thomsonrights.com

Library of Congress Cataloging-in-Publication Data:

Pardoe, Terry D.
Network security / Terry Pardoe, Gordon Snyder.
p. cm.
Includes index.
ISBN 1-4018-8214-5
1. Computer networks—Security measures. I. Snyder, Gordon. II. Title.

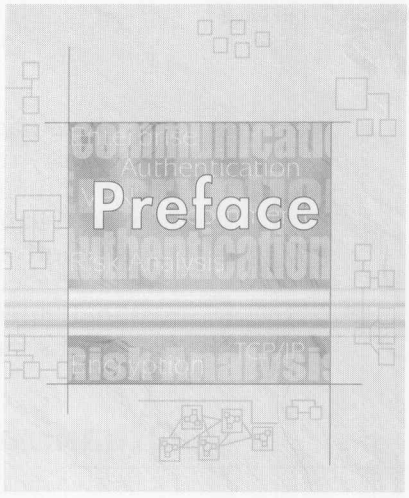
TK5105.59.P38 2005
005.8—dc22 2004051697

NOTICE TO THE READER

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims,any obligation to obtain and include information other than that provided to it by the manufacturer.

The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions.

The Publisher makes no representation or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.



Audience

This book is designed as a first-year introductory network security text for telecommunications and information technology students interested in learning about the networking and security fields. The text has been written at a basic introductory level for students, providing a good overview of security issues and their contemporary solutions without delving too deeply into any one topic. Prerequisites are minimal and a computer hardware and software (for example, A+) and networking (for example, Network+) background will suffice. It has been designed for the freshman level electronics engineering, electronics technology, computer information systems, and computer science student who has not taken advanced mathematics or electronics courses. It is hoped that, after completing the text, students' interest in networks and security will be sparked, and they will want to learn more about security techniques and technologies. Because of the general nature of the text, this material is also a valuable resource to business students who need to broaden their knowledge of computer systems and the potential risks involved in their business use.

Approach

The text gives basic coverage of computer hardware, operating systems, and network technologies. A more detailed presentation of both security risks and practical solutions follows this introduction, together

with design and operational hints that the authors believe are invaluable. Topics are introduced at a basic level and covered without a lot of heavy mathematics, and the intended result is to interest students in network security, business system security, and other security issues and to motivate them to take additional higher-level courses. The text provides practical examples of theory, using mathematics only when required, and students will finish with a good understanding of all aspects of security issues and solutions.

Organization

As computer systems have evolved from the early teleprocessing-based approach to today's complex, enterprise-wide, client/server solutions, the security risks and the possible protective measures have also become complex. The text covers a wide range of past and present issues and aims to ensure that students leave with a good understanding of how and why things have changed in the past, and where we are today in preparation for changes that will continue into the future. The material covered is organized into five parts.

Part One is an introduction to computer technology and networking. It lets us understand the computer environment and the technologies that support it and how we have progressed to today's complex, network-based, interactive business and personal systems. It provides an excellent background of the factors that impact both computer and network security.

Chapter 1 reviews the history of computer use and shows how issues surrounding security have become more and more important as we progressed from simple mainframe-based systems to today's client/server-based implementations.

Content follows the progression from considering the computer and its applications as a simple business utility support to the use of computer systems as tactical weapons in the competitive battle for customers, clients and the minds of citizens.

Chapter 2 guides us through the development and use of operating systems and indicates how they are used, not only as the supervisor of the machines and their resources, but also as the basis on which much of a system's security controls are built. We show how simple and complex application programs build on these services to create their own security controls.

The Internet and the World Wide Web have become an integral part of both personal and business solutions, and we have introduced the range of security issues brought about by this type of networking.

Chapter 3 explores in detail all aspects of computer networking in order that we may understand the impact of interconnection on system performance, reliability, and security. The topology and deployment of various network types is discussed to deepen our insight into where things are and who has access to them as they relate to overall asset risk and security need. We pay particular attention to the ISO/OSI reference model because of its importance as the basis of modern networking and because we use its format within later chapters.

Chapter 4 deals in-depth with the technical aspects of local area network technology. Local area networks are the most popular way of delivering computational services to the end user in government, business, and academic environments. They also represent a portion of any system solution that is both exposed to illicit attack and can define the basic performance of a business solution. We concentrate on the various forms of Ethernet, an open, broadcast technology, because it is the most commonly used. We briefly discuss such technologies as token ring, because their use is rapidly diminishing in the business world.

Chapter 5 discusses the TCP/IP protocols, which have become the de facto standard for all networking, and the increasingly popular use of Internet technology both inside a corporation and across the globe. While TCP/IP-based networks have a well-founded reputation for being insecure, their heavy use demands that we understand their operation in detail if we are to build and operate secure systems using this type of technology. Furthermore, the success of both consumer-to-business and business-to-business electronic commerce relies, in part, on the availability and low cost of the public Internet, which requires a good understanding of this type of connection and the wide range of vulnerabilities to illicit use it presents.

Part Two defines and discusses the general environment within which security issues are assessed, categorized, prioritized, and evaluated in terms of financial and general business losses. We stress the importance of assessing risks and, because it is people who directly or indirectly attack our business systems, the importance of understanding how humans and other programs are identified and authenticated.

Chapter 6 concentrates on risk and threat analysis. We introduce a project management approach to this analysis because extensive reviews of human efforts have revealed, consistently, that success is maximized if careful planning and formal methodology are used, rather than "taking the ball and running with it." Additionally we believe that it is essential that the nature of computer crime must be understood before effective analysis of risk can be made. Similarly we discuss the tools of the computer criminal, even at this early stage, to help in the understanding of the risks our systems face and their possible impact. We also recognize that special risks are attendant on the

use of the public Internet or the use of Internet technology within internal corporate networks, and we address and explain these issues as part of the analysis process. Analyses, plans, and approaches have to be "sold" to management, so we round out this chapter with comments on making good presentations.

Chapter 7 concentrates on the important topic of the human beings who use computer systems. We emphasize that it is human beings who represent the source of all problems and that, as such, it is important that system users be recognized and authenticated before they can access resources or manipulate corporate or personal information. Since the traditional way to recognize a human is by some form of password, we spend time defining good versus bad types of passwords and a range of ways of improving password generation and usage. Passwords alone are not sufficient for controlling access to sensitive systems, so we additionally describe a range of authentication tools that make the recognition of an individual more certain. Such techniques as the use of tokens and biometrics are introduced to reinforce the idea that strong authentication is possible when needed.

Part Three details the technology needed to secure systems from many forms of attack and describes both software and hardware approaches to controlling system access, abuse, misuse, and destruction. We fully understand that the last word on technology has yet to be written, so we concentrate on defining and describing the major approaches to enhance the general understanding of the tools that are available today and anticipated tomorrow, which can be used to prevent a wide range of system attacks.

Chapter 8 presents basic information on encryption for data protection as well as a fuller explanation of the operation of such things as smart tokens and biometrics for access control and authentication. We describe the implementation of single-key and multiple-key encryption and describe the advantages and limitations of each approach. A general understanding of these techniques is essential to a fuller understanding of other, more complex tools used to fight off the would-be attacker and protect essential data. We also describe the processes used to create digital signatures, which are used to validate that the contents of a transmission have not been altered after creation, and certificates of authentication to validate the authorship. We explain how many services can be implemented in both hardware or software, and provide the logic for making the decision as to which should be used. Using these basic technologies we describe the use and operation of many token-based systems and biometrics recognition devices and their value and limitations.

Chapter 9 uses the ISO/OSI model to provide a basis for our understanding of the use of a range of protocols to provide secure transmission of data at the detailed physical, bit-by-bit, level through the network layer. A good understanding of these techniques is essen-

tial to the operation, for example, of a simple telephone/modem connection for data transfer. We emphasize the use of such protocols as point-to-point tunneling protocol to provide an essential basis for the proper operation of virtual private networks, private networks operating "on top of" public networks, and other secure low-level transfers. The network layer of a TCP/IP-based network uses a protocol called Internet protocol (IP), and considerable changes have been made to the specification in the latest version to improve security across a network, so we explain these changes and where they are leading.

Chapter 10 provides information on security issues at the upper (ISO) layers; that is, security vulnerabilities based on specific application usages. After reviewing a range of well-established ways in which TCP/IP systems have been attacked, and suggesting solutions, we describe the basic operation of the Internet and internal intranets.

An understanding of these technologies is important, as they are often combined in today's business or government systems. The inclusion of the public and open Internet in a business system brings with it an ideal "way in" for would-be attackers. We therefore concentrate our efforts in two areas: the protection of the internal network from outsiders and the types of things we are attempting to protect against. This approach means we first define and describe a range of firewall approaches that can be implemented to keep the attackers out, and then we discuss a wide range of attacker tools. Viruses, worms, denial-of-service attacks, and the use of e-mail as a technique to bypass other controls are described in detail, and a wide range of solutions is offered.

Part Four considers a wide range of complex systems and then proceeds to formalize both the planning and design of complex solutions and their installation and long-term operation. Again we provide a formal process for these important steps to help ensure that errors are not made. We emphasize that solutions are what is expected and, more importantly, needed.

Chapter 11 reviews a range of complex systems used in business and government environments. E-commerce is described in full, as well as the risks involved and their possible solutions. This requires a full understanding of the operation of World Wide Web technology and the protective measures that have been created within it. We describe secure operation of Web page transfer and the more sophisticated application of such approaches as secure socket layer and secure electronic transaction to enhance the knowledge of how business processes are protected and indicate where the risks reside. We also consider the growing use of cellular-phone–based wireless systems and the special nature of creating a secure environment in a broadcast system. In today's business arena many systems span the entire enterprise, and we review applications such as decision support systems,

where the risks are based on the misuse of information, and data mining, where the risks may be more a privacy issue than an attack issue.

Chapter 12 concentrates on the proper design and installation of a complex system. We present a detailed approach to the design process specifically to prevent errors of omission and false expectations or a false sense of security.

We recognize that the design of all systems follows some form of system design life cycle methodology and, rather than emphasize the use of a particular method, we use a general approach and concentrate on aspects that are of specific concern when attempting to create a secure system. We pay special attention to planning needs, the use of external contractors, and the essential tasks of continuous and final testing. For completeness, we add information on loss insurance for complex systems.

Chapter 13 addresses the issues of long-term operation. Support is an essential component of any system. When things go wrong and professional help is needed, it must be available. If it is not, enthusiastic business users start to break the rules. The classical situation of "my account doesn't work . . . let me have your password" defeats the protective aspects of any system quickly. We detail the type of staffing needed to operate an effective help desk and eliminate such problems. Proper operation also requires the perpetuation of originally promised or proven support. We see this as a security aspect since poor performance encourages "cheating," so we explain the processes needed and the software support required to monitor performance.

Additionally we present details of how illegal intrusion attempts should be monitored and tracked. We define how third parties can be used to periodically test the integrity of systems.

Part Five explores the future.

Chapter 14 shows where future attacks may come from and their most likely form. We also describe the types of technology that are evolving to protect against such attacks. Understanding the future is the best way to stay safe. We also provide extensive information on where to find both current and future information, support, and advice.

Features

- Information is presented in plain text, allowing readers to make immediate connections between theory and practice.
- Examples and illustrations focus exclusively on network concepts and security issues and solutions, without straying into side topics.

- Objectives, outlines, key terms, summaries, and review questions in every chapter focus attention on key concepts and speed learning.
- End-of-text glossary includes acronyms and gives students a quick reference to basic terms used in the computer, telecommunications, and security industries.
- Information is accessible to technology and business students and readers without higher-level math skills or detailed knowledge of networking.

Supplements

Instructor's Manual

- End-of-chapter solutions and answers
- PowerPoint instructor materials
- Notes on additional workshops and projects
- Sample tests and final exams
- Sample course outlines

On-line Companion

See the *Network Security* On-line WebTutor at *http://e.thomsonlearning.com* for up-to-date information on a wide range of evolving security issues, extensive project information, and a detailed list of Web links on all topics covered in the book.

Acknowledgments

The authors would like to thank the following individuals whose vision and insight helped to provide the motivation for development of this text. From the National Science Foundation: Program Officers Elizabeth Teles and Gerhard Salinger; from Springfield Technical Community College: President Andrew Scibelli, Vice President Stephen Keller, Foundation Press Executive Director Debbie Bellucci and Professor Diane D. Snyder; from the National Center for Telecommunications Technologies (NCTT) at Springfield Technical Community College: Gary Mullett, James Downing, Nina Laurie, Joseph Joyce, Helen Wetmore, Scott SaintOnge, Fran Smolkowicz, and retired NCTT

Executive Director James Masi. We also sincerely thank Susan V. Pardoe, Penny S. Pardoe, and the faculty of the New Hampshire Community Technical College–Nashua, and the staff of various U.S. government agencies, too numerous to list, who have supported the efforts of T. D. Pardoe over the last thirty years. Without the help of each, this text would never have been completed.

The following have reviewed the text and have provided valuable input: Anne Cox, Austin Community College, Austin, TX; David DiFabio, Pittsburgh Technical Institute, Oakdale, PA; Reda Elias, DeVry University, Chicago, IL; Charles Lange, DeVry University, N. Brunswick, NJ; Judson Miers, DeVry University, Kansas City, MO; David Oveissi, DeVry University, Arlington, VA; Marsha Powell, Tompkins Cortland Community College, Dryden, NY; Eric Salveggio, Virginia College, Birmingham, AL; Brent Williams, Purdue University, West Lafayette, IN.

Gordon Snyder would also like to thank his wife, Diane, and children, Eva and Gabby, for understanding that these things take so much time!

NCTT

The National Center for Telecommunications Technologies (NCTT) is a National Science Foundation (NSF)-sponsored Advanced Technological Education (ATE) Center, established in 1997 by Springfield Technical Community College (STCC: *www.stcc.edu*) and the National Science Foundation. All material produced as part of the NCTT textbook series is based on work supported by the Springfield Technical Community College and the National Science Foundation under Grant Number DUE 9751990.

NCTT was established in response to the telecommunications industry and the worldwide demand for instantly accessible information. Voice, data, and video communications across a worldwide network are creating opportunities that did not exist a decade ago, and preparing a workforce to compete in this global marketplace is a major challenge for the Information and Communications Technology (ICT) and ICT-enabled industries. As we enter the twenty-first century, with even more rapid breakthroughs in technology anticipated, education is the key, and NCTT is working to provide the educational tools employers, faculty, and students need to keep the United States competitive in this evolving industry.

We encourage you to visit the NCTT Web site at *www.nctt.org,* along with the NSF Web site at *www.nsf.gov,* to learn more about this and other exciting projects. Together we can explore ways to better

prepare quality technological instruction and ensure the globally competitive advantage of America's ICT and ICT-enabled industries.

About the Authors

Terry D. Pardoe

Terry Pardoe was born in the United Kingdom and graduated from the Birmingham College of Advanced Technology (now Aston University) with a major in Applied Physics. He was executive vice president of International Management Services Inc., a U.S.-based computer application and training organization, for twenty-three years (until August 1999). He has more than thirty years of experience in the design and application of information systems.

Mr. Pardoe is a recognized expert on all aspects of telecommunication and networking, including wide and local area networks, TCP/IP-based networks, the Internet, intranets, client/server computing, data and network security, and many other applied areas. He has lectured and consulted on a worldwide basis for a wide range of clients, including: Digital Equipment Corp., AT&T, Sprint United, Citibank, IBM, Honeywell, NT&T (Hong Kong), and SCI (Brazil), and others. He has worked with all major agencies of the U.S. government, including: NASA, NSA, DISA, U.S. Navy, U.S. Army, IRS, and many others.

Mr. Pardoe is the author or co-author of more than two hundred privately published technical training manuals on computer applications, management techniques, and data communications, including text to support the first Java seminar available on a worldwide basis. He has authored many Web pages that include complex graphics, Java applets, and JavaScript. Since 1999 Mr. Pardoe has been a part-time lecturer at New Hampshire Community Technical College–Nashua and a subject-matter-expert trainer in the Verizon Next Step program.

Gordon F. Snyder, Jr.

Gordon F. Snyder, Jr. is executive director and principal investigator for NCTT at Springfield Technical Community College (STCC), where he also serves as project director of the *Microsoft Working Connections* grant program and manages curriculum development for networking. He has taught in the telecommunications, electronics systems, computer systems, and laser electro-optics departments at STCC since 1984, and cochaired those departments from 1990 to 1999. He helped

develop the Verizon Next Step program and now serves as the New England telecommunications curriculum coordinator for the Verizon Next Step program. He was an adjunct instructor in the bioengineering department at Western New England College and is the author of two other engineering textbooks. He has extensive consulting experience in the field of communications and LAN/WAN design. He has served on several local and national boards, including the Massachusetts Telecommunictions Council, the Microsoft Community & Technical College Advisory Council, and the National Skill Standards Board (NSSB) Information and Communications Technology (ICT) Voluntary Partnership representing the telecommunications, computer, and information industry sector. In March of 2004 he was presented with the Massachusetts Telecommunications Council Workforce Development Award, and in 2001 he was selected as one of the top fifteen technology faculty in the United States by the American Association of Community Colleges and Microsoft Corporation.

Mr. Snyder received dual bachelor of science degrees in microbiology and medical technology from University of Massachusetts–Amherst, and the master of science in electrical engineering from Western New England College.

To my wife Susan, with gratitude for her patience and understanding

—Terry Pardoe

Dedicated to my wife Diane and daughters Eva and Gabby

—Gordon Snyder