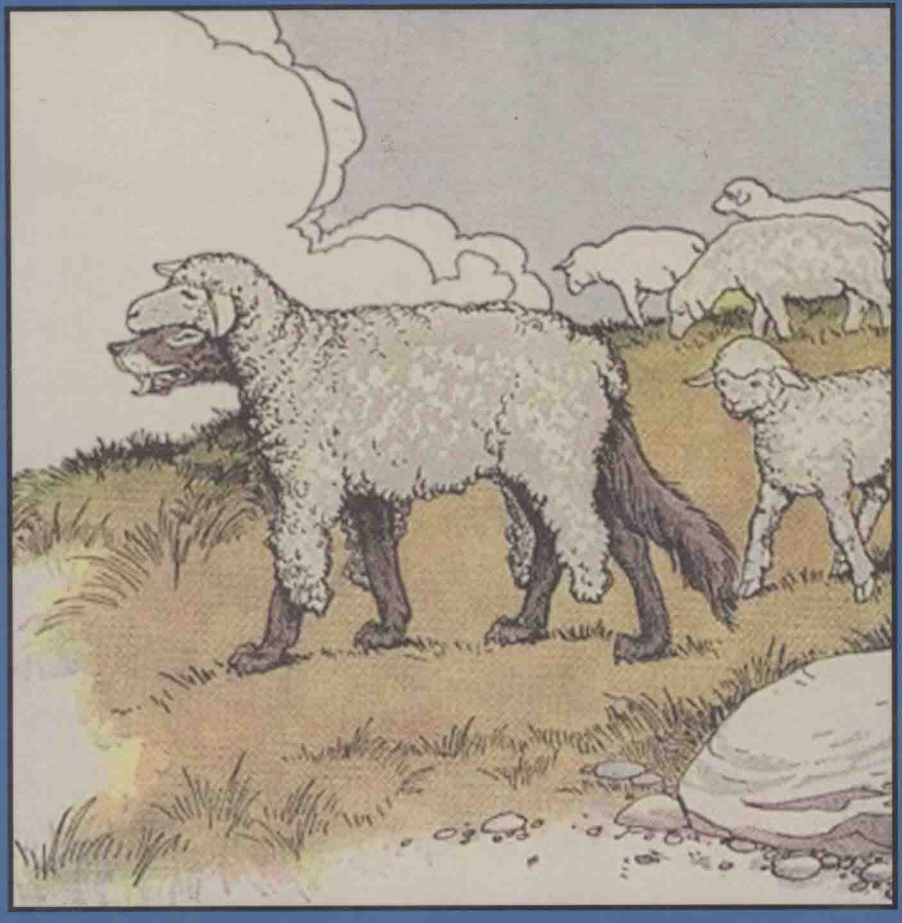
CHAPMAN & HALL/CRC COMPUTER and INFORMATION SCIENCE SERIES

Introduction to Network Security



Douglas Jacobson

CRC Press
Taylor & Francis Group

Introduction to Network Security

江苏工业学院图书馆
藏书章

Douglas Jacobson
Iowa State University
Ames, Iowa, U.S.A.

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2009 by Taylor & Francis Group, LLC
Chapman & Hall/CRC is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-58488-543-6 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Jacobson, Douglas.
Introduction to network security / Douglas Jacobson.
p. cm. -- (Chapman and Hall/CRC computer and information science series)
Includes bibliographical references and index.
ISBN 978-1-58488-543-6 (hbk. : alk. paper)
1. Computer networks--Security measures. 2. Computer security. I. Title. II. Series.

TK5105.59.J33 2008
005.8--dc22 2008040768

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Introduction to Network Security

CHAPMAN & HALL/CRC
COMPUTER and INFORMATION SCIENCE SERIES

Series Editor: Sartaj Sahni

PUBLISHED TITLES

ADVERSARIAL REASONING: COMPUTATIONAL APPROACHES TO READING THE OPPONENT'S MIND
Alexander Kott and William M. McEneaney

DISTRIBUTED SENSOR NETWORKS
S. Sitharama Iyengar and Richard R. Brooks

DISTRIBUTED SYSTEMS: AN ALGORITHMIC APPROACH
Sukumar Ghosh

FUNDEMENTALS OF NATURAL COMPUTING: BASIC CONCEPTS, ALGORITHMS, AND APPLICATIONS
Leandro Nunes de Castro

HANDBOOK OF ALGORITHMS FOR WIRELESS NETWORKING AND MOBILE COMPUTING
Azzedine Boukerche

HANDBOOK OF APPROXIMATION ALGORITHMS AND METAHEURISTICS
Teofilo F. Gonzalez

HANDBOOK OF BIOINSPIRED ALGORITHMS AND APPLICATIONS
Stephan Olariu and Albert Y. Zomaya

HANDBOOK OF COMPUTATIONAL MOLECULAR BIOLOGY
Srinivas Aluru

HANDBOOK OF DATA STRUCTURES AND APPLICATIONS
Dinesh P. Mehta and Sartaj Sahni

HANDBOOK OF DYNAMIC SYSTEM MODELING
Paul A. Fishwick

HANDBOOK OF PARALLEL COMPUTING: MODELS, ALGORITHMS AND APPLICATIONS
Sanguthevar Rajasekaran and John Reif

HANDBOOK OF REAL-TIME AND EMBEDDED SYSTEMS
Insup Lee, Joseph Y-T. Leung, and Sang H. Son

HANDBOOK OF SCHEDULING: ALGORITHMS, MODELS, AND PERFORMANCE ANALYSIS
Joseph Y.-T. Leung

HIGH PERFORMANCE COMPUTING IN REMOTE SENSING
Antonio J. Plaza and Chein-I Chang

INTRODUCTION TO NETWORK SECURITY
Douglas Jacobson

PERFORMANCE ANALYSIS OF QUEUING AND COMPUTER NETWORKS
G. R. Dattatreya

THE PRACTICAL HANDBOOK OF INTERNET COMPUTING
Munindar P. Singh

SCALABLE AND SECURE INTERNET SERVICES AND ARCHITECTURE
Cheng-Zhong Xu

SPECULATIVE EXECUTION IN HIGH PERFORMANCE COMPUTER ARCHITECTURES
David Kaeli and Pen-Chung Yew

此为试读，需要完整PDF请访问：www.ertongbook.com

Preface

Approach

This book focuses on network security from the viewpoint of a network's vulnerabilities, protocols, and security solutions. Unlike other books that focus on security and security paradigms where networks are viewed as a mechanism for communication, this book focuses on the network as a source of both insecurity and security. The book will examine various network protocols looking at vulnerabilities, exploits, attacks, and methods to mitigate an attack.

Networks as communication systems have been around since the dawn of human history and rely on trust between communicating parties in order to function. Early communications systems relied on visual verification of the communicating parties involved and often used simple codes to protect the data. For example, couriers were known by both parties and messages were sealed with wax to help ensure privacy. As technology improved, methods used to transmit data also improved, and so did the methods to steal and protect data. However, even as late as the end of the twentieth century, data was still being transmitted directly between two parties with no concept of a network. These parties relied on additional knowledge to verify the authenticity of the data. The issues we face today are more complex than those of the past. Today we have interconnected computers using a network not controlled by any one entity or organization. Unlike data communications of the past, today's networks consist of numerous devices that handle the data as it passes from the sender to the receiver. These networks are designed to facilitate communication and are intended for a small group of trusted and knowledgeable individuals. Security is not part of the design process.

Organization

Part I of this book is a brief discussion of network architectures and the functions of layers in a typical network, along with a taxonomy of network-based vulnerabilities and attacks. This taxonomy is the framework for presenting the vulnerabilities and attacks at each layer of interest. The taxonomy divides the

vulnerabilities and attack space into four categories:

Header-based vulnerabilities and attacks: The protocol headers have been modified or are not valid.
Protocol-based vulnerabilities and attacks: The packets are valid but are not used correctly.
Authentication-based vulnerabilities and attacks: The identity of the sender or receiver is modified.
Traffic-based vulnerabilities and attacks: The volume of traffic creates the attack.

The remainder of the book is divided into three parts. Part II covers the different layers of the network (physical, network, and transport), looking at the security for each. Using a bottom-up approach to network security allows the reader to understand the vulnerabilities and the security mechanisms provided by each layer of the network. For example, by understanding which vulnerabilities are introduced by the physical layer and what level of security can be provided, the reader can understand which vulnerabilities may exist in the network layer and which security mechanisms could be used to overcome the vulnerabilities. Part III looks at the security of several common network applications. On the Internet, applications treat the lower layers of the network as a simple pipe that sends data to another application, and it arrives without error. This book views vulnerabilities as network functions provided by the layer below, thus giving the reader insight into understanding the security needed to overcome the vulnerabilities. Part IV provides an overview of several network-based security solutions that are often deployed and relates them back to the taxonomy.

This book describes a define–attack–defend methodology for network security. The relevant protocols are briefly introduced, followed by detailed descriptions of known vulnerabilities and possible attack methods. The book then focuses on the attack methodology rather than on particular tools, though tools are introduced as possible homework problems and lab experiments. Once the reader understands the threats against the protocol, possible solutions will be presented. Each chapter has homework problems that are based on the concepts introduced in the chapter and will have lab experiments that will allow the reader to try some of the attacks and look at the effectiveness of the solutions. An appendix provides details to develop and deploy a low-cost lab environment that can be used to support the classroom or used as a small corporate test bed. Another appendix provides an overview to cryptology.

Target Audience

This book is targeted at two compatible audiences. The primary focus of the book is as a text for a senior or first-year graduate course in network security for students in computer science or computer engineering. The book can be used for a network security course that is part of a security curriculum or for a course that is part of a networking curriculum. The book is also intended as a reference for network and security professionals.

Differences between this book and other books include:

Network focused: This book looks at network security by exploring network protocols, their weaknesses, and countermeasures. Several books also have a network focus but primarily deal with a few application-level protocols (Kerberos, secure email, secure web, etc.) and are not concerned about the lower layers (physical, network, transport). Many of the difficult problems arise from the vulnerabilities in these layers.

Network view of security: This book looks at network security using the approaches found in most network books, by looking at the layers and what services and functions are provided. We will look at vulnerabilities and security as services and functions provided by the layer. By using a network view, the book could be used in either a networking curriculum to add security or in a security curriculum to add network security.

Lab experiments: This book contains lab experiments to support the material. The experiments will look at both attacks and defenses. The book also provides a low-cost lab configuration that can be used as a model.

Web site: A web site is provided to support the book (http://www.dougj.net/textbook/). The web site contains lecture materials, tutorials on UNIX, C, and socket programming, and detailed information to establish and maintain the test laboratory.

Practical view of network security: This book has a practical view of network security. We will look at actual protocols and provide readers with the details and information they need to understand

the vulnerabilities and to develop appropriate countermeasures. This is reinforced through the lab experiments.

Attack-and-defend approach: This book looks at network security from an attack-and-defend approach. The book looks at the vulnerabilities in the current protocols and then looks at defense systems that could mitigate the attacks. While the book will not focus on attack tools, it will look at attack methods, and through the lab experiments, students will be able to study the effects of certain attacks on the network and the effectiveness of the security system.

Terms defined: So much of networking and security involves the use of terms, many of which are specific to the field. Thus, I feel that it is important after each section of a chapter to enumerate with a short definition any new terms that were defined in that section. Before we begin the text, there are a few terms that should be defined so readers have a common frame of reference.

Definitions

Application.
A computer program that allows a user to connect to the network and perform a task.

Attacker.
A person or persons that use the network to attack computer systems, networks, or other devices connected to the Internet.

Hacker.
Same as an attacker.

Host.
A term used to describe a computer connected to the Internet.

Internet.
A global collection of networks of interconnected network devices.

Network.
A group of interconnected devices that can communicate with each other.

Network device.
A device connected to the network. This is more generic than a host or computer in that it can be any network-enabled device.

Target.
The device, host, user, or object that the hacker is trying to attack.
User.
The individual using a computer application that utilizes the network, or a general computer user.

Acknowledgments

I thank my wife, Gwenna, and my children (Sarah, Jordan, and Jessica) for all of their support and patience. I also thank Sharon Sparks for her editing help.

此为试读,需要完整PDF请访问: www.ertongbook.com

The Author

Doug Jacobson is a university professor in the Department of Electrical and Computer Engineering at Iowa State University. He is currently director of the Iowa State University Information Assurance Center, which has been recognized by the National Security Agency as a charter Center of Academic Excellence for Information Assurance Education. Dr. Jacobson teaches network security and information warfare. He also works with local law enforcement and is a computer forensics analyst for the Iowa State University Police Department. Dr. Jacobson is the founder of Palisade Systems, Inc., an Ames-based company marketing Internet management and security devices. He has received two R&D 100 awards for his security technology and has two patents in the area of computer security.

Contents

此为试读,需要完整PDF请访问: www.ertongbook.com