SECOND EDITION

Foundations of Cybersecurity

A Straightforward Introduction

Jason Andress

Previously *Foundations of Information Security*

no starch press®

SECOND EDITION

Foundations of Cybersecurity

A Straightforward Introduction

Jason Andress

Previously *Foundations of Information Security*

no starch press®

FOUNDATIONS OF CYBERSECURITY

2nd Edition

A Straightforward Introduction

by Jason Andress

no starch
press®

San Francisco

First printing

30 29 28 27 26 1 2 3 4 5

ISBN-13: 978-1-7185-0440-0 (print)

ISBN-13: 978-1-7185-0441-7 (ebook)

Published by No Starch Press®, Inc.

245 8th Street, San Francisco, CA 94103

phone: +1.415.863.9900

www.nostarch.com; info@nostarch.com

Publisher: William Pollock

Managing Editor: Jill Franklin

Production Manager: Sabrina Plomitallo-González

Production Editor: Jennifer Kepler

Developmental Editor: Frances Saux

Cover Illustrator: Rick Reese

Interior Design: Octopod Studios

Technical Reviewer: Steve Winterfeld

Copyeditor: Sharon Wilkey

Proofreader: Cindy Snyder

Indexer: BIM Creatives, LLC

Library of Congress Control Number for the first edition: 2019024099

For customer service inquiries, please contact info@nostarch.com. For information on distribution, bulk sales, corporate sales, or translations: sales@nostarch.com. For permission to translate this work: rights@nostarch.com. To report counterfeit copies or piracy: counterfeit@nostarch.com. The authorized representative in the EU for product safety and compliance is EU Compliance Partner, Pärnu mnt. 139b-14, 11317 Tallinn, Estonia, hello@eucompliancepartner.com, +3375690241.

Perseverantia omnia vincit.

About the Author

Dr. Jason Andress is a veteran security professional and security researcher with deep expertise across the cybersecurity landscape. His work spans topics such as data protection, network defense, hardware security, penetration testing, and digital forensics.

About the Technical Reviewer

Steve Winterfeld has worked many cybersecurity jobs, from penetration tester to CISO. Today, he provides expert cybersecurity consulting and has a track record of building operational and compliance-driven security programs at both the strategic and tactical levels.

BRIEF CONTENTS

Acknowledgments

Introduction

PART I: CORE PRINCIPLES

Chapter 1: What Is Cybersecurity?

Chapter 2: The Threat Landscape

Chapter 3: Identification and Authentication

Chapter 4: Authorization and Access Controls

Chapter 5: Auditing and Accountability

Chapter 6: Cryptography

PART II: ARCHITECTURE, INFRASTRUCTURE, AND SYSTEM SECURITY

Chapter 7: Security Architecture

Chapter 8: Network Security

Chapter 9: Operating System Security

Chapter 10: Mobile, Embedded, and Internet of Things Security

Chapter 11: Application Security

Chapter 12: AI Security

PART III: SECURITY OPERATIONS AND MANAGEMENT

Chapter 13: SecOps, the SOC, and Incident Response

Chapter 14: Governance, Risk, and Compliance

Chapter 15: Vulnerability Assessments and Penetration Testing

PART IV: HUMAN FACTORS AND PROFESSIONAL DEVELOPMENT

Chapter 16: Social Engineering

Chapter 17: Security Awareness

Chapter 18: So You Want to Be a Security Professional

Notes

Index

CONTENTS IN DETAIL

ACKNOWLEDGMENTS

INTRODUCTION

Who Should Read This Book?

What's New in This Edition?

About This Book

PART I
CORE PRINCIPLES

1
WHAT IS CYBERSECURITY?

Defining Cybersecurity

When Are You Secure?

Models for Discussing Security Issues

The Confidentiality, Integrity, and Availability Triad

The Parkerian Hexad

Attacks

Classification of Attacks

Threats, Vulnerabilities, and Risks

Defense in Depth

Summary

Review Questions

Project #1: Testing Password Entropy

2
THE THREAT LANDSCAPE

State Actors

Intergovernmental Organizations

State-Sponsored Actors

Non-State Actors

Security Researchers

Corporations

Criminal Groups

Malware Authors

Hacktivists and Patriot Hackers

Autonomous Actors

Attribution

Threat Actor Skill Levels

Summary

Review Questions

Project #2: Classifying Edward Snowden

3
IDENTIFICATION AND AUTHENTICATION

Identification

Who We Claim to Be

Identity Verification

Identity Falsification

Authentication

Factors

Multifactor Authentication

Mutual Authentication

Common Identification and Authentication Methods

Passwords

Biometrics

Hardware Tokens

Summary

Review Questions

Project #3: Hashing Passwords

4
AUTHORIZATION AND ACCESS CONTROLS

What Are Access Controls?

Implementing Access Controls

Access Control Lists

Capabilities

Access Control Models

Discretionary

Mandatory

Rule-Based

Role-Based

Attribute-Based

Multilevel

Physical Access Controls

Summary

Review Questions

Project #4: Finding Confused Deputies in the Wild

5
AUDITING AND ACCOUNTABILITY

Accountability

Security Benefits of Accountability

Nonrepudiation

Deterrence

Intrusion Detection and Prevention

Admissibility of Records

Auditing

Choosing What to Audit

Logging

Monitoring

Auditing with Assessments

Summary

Review Questions

Project #5: Working with Audit Logs

6
CRYPTOGRAPHY

The History of Cryptography

The Caesar Cipher

Cryptographic Machines

Kerckhoffs's Principles

Modern Cryptographic Tools

Keyword Ciphers and One-Time Pads

Symmetric and Asymmetric Cryptography

Hash Functions

Digital Signatures

Certificates

Protecting Data at Rest, in Motion, and in Use

Protecting Data at Rest

Protecting Data in Motion

Protecting Data in Use

Summary

Review Questions

Project #6: Encrypting and Decrypting with PGP

PART II
ARCHITECTURE, INFRASTRUCTURE, AND SYSTEM SECURITY

7
SECURITY ARCHITECTURE

A City Planning Metaphor

Structure, Patterns, and Intent

Built-in vs. Bolted-on Security

Foundational Architectural Principles

Least Privilege

Separation of Duties

Secure Defaults

Simplicity and Clarity

Zero Trust

Layered Design

Trust Boundaries

Defining Security Zones

Designing with Boundaries in Mind

Risk-Driven Architecture

Risk Scoring

Risk Tiers

Threat Modeling

Frameworks for Enterprise Security Architecture

Summary

Review Questions

Project #7: Assessing a Real Security Architecture

8
NETWORK SECURITY

Protecting Networks

Designing Secure Networks

Using Firewalls

Implementing Network Intrusion Detection Systems

Protecting Network Traffic

Using Virtual Private Networks

Protecting Data over Wireless Networks

Using Secure Protocols