INFORMATION SECURITY

PRINCIPLES AND PRACTICES

SECOND EDITION

MARK S. MERKOW • JIM BREITHAUPT

Information Security: Principles and Practices

Second Edition

Mark S. Merkow
Jim Breithaupt

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Information Security: Principles and Practices

Table of Contents

Table of Contents
Preface
Chapter 1: Why Study Information Security?
- Introduction
- The Growing Importance of IT Security and New Career Opportunities
  - An Increase in Demand by Government and Private Industry
- Becoming an Information Security Specialist
  - Schools Are Responding to Demands
  - The Importance of a Multidisciplinary Approach
- Contextualizing Information Security
  - Information Security Careers Meet the Needs of Business
- Summary
- Test Your Skills

Chapter 2: Information Security Principles of Success
- Introduction
- Principle 1: There Is No Such Thing As Absolute Security
- Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability
  - Integrity Models
  - Availability Models
- Principle 3: Defense in Depth as Strategy

Table of Contents

Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

Principle 6: Security Through Obscurity Is Not an Answer

Principle 7: Security = Risk Management

Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

Principle 9: Complexity Is the Enemy of Security

Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

Summary

Test Your Skills

Chapter 3: Certification Programs and the Common Body of Knowledge

Introduction

Certification and Information Security

International Information Systems Security Certifications Consortium (ISC)([Sup2])

The Information Security Common Body of Knowledge

Information Security Governance and Risk Management

Security Architecture and Design

Business Continuity and Disaster Recovery Planning

Legal Regulations, Investigations, and Compliance

Table of Contents

Physical (Environmental) Security

Operations Security

Access Control

Cryptography

Telecommunications and Network Security

Software Development Security

Other Certificate Programs in the IT Security Industry

Certified Information Systems Auditor

Certified Information Security Manager

Certified in Risk and Information Systems Control

Global Information Assurance Certifications

(ISC)([Sup2]) Specialization Certificates

CCFP: Certified Cyber Forensics Professional

HCISPP: HealthCare Information Security and Privacy Practitioner

Vendor-Specific and Other Certification Programs

Summary

Test Your Skills

Chapter 4: Governance and Risk Management

Introduction

Security Policies Set the Stage for Success

Understanding the Four Types of Policies

Programme-Level Policies

Programme-Framework Policies

Issue-Specific Policies

System-Specific Policies

Developing and Managing Security Policies

Security Objectives

Operational Security

Policy Implementation

Table of Contents

- Providing Policy Support Documents
  - Regulations
  - Standards and Baselines
  - Guidelines
  - Procedures
- Suggested Standards Taxonomy
  - Asset and Data Classification
  - Separation of Duties
  - Employment Hiring Practices
  - Risk Analysis and Management
  - Education, Training, and Awareness
- Who Is Responsible for Security?
- Summary
- Test Your Skills

Chapter 5: Security Architecture and Design

- Introduction
- Defining the Trusted Computing Base
  - Rings of Trust
- Protection Mechanisms in a TCB
- System Security Assurance Concepts
  - Goals of Security Testing
  - Formal Security Testing Models
- The Trusted Computer Security Evaluation Criteria
  - Division D: Minimal Protection
  - Division C: Discretionary Protection
  - Division B: Mandatory Protection
  - Division A: Verified Protection
  - The Trusted Network Interpretation of the TCSEC

Table of Contents

The Information Technology Security Evaluation Criteria

Comparing ITSEC to TCSEC

ITSEC Assurance Classes

The Canadian Trusted Computer Product Evaluation Criteria

The Federal Criteria for Information Technology Security

The Common Criteria

Protection Profile Organization

Security Functional Requirements

Evaluation Assurance Levels

The Common Evaluation Methodology

Confidentiality and Integrity Models

Bell-LaPadula Model

Biba Integrity Model

Advanced Models

Summary

Test Your Skills

Chapter 6: Business Continuity Planning and Disaster Recovery Planning

Introduction

Overview of the Business Continuity Plan and Disaster Recovery Plan

Why the BCP Is So Important

Types of Disruptive Events

Defining the Scope of the BCP

Creating the Business Impact Analysis

Disaster Recovery Planning

Identifying Recovery Strategies

Understanding Shared-Site Agreements

Table of Contents

- Using Alternate Sites
- Making Additional Arrangements
- Testing the DRP

Summary

Test Your Skills

Chapter 7: Law, Investigations, and Ethics

Introduction

Types of Computer Crime

How Cybercriminals Commit Crimes

The Computer and the Law

- Legislative Branch of the Legal System
- Administrative Branch of the Legal System
- Judicial Branch of the Legal System

Intellectual Property Law

- Patent Law
- Trademarks
- Trade Secrets

Privacy and the Law

- International Privacy Issues
- Privacy Laws in the United States

Computer Forensics

The Information Security Professionals Code of Ethics

Other Ethics Standards

- Computer Ethics Institute
- Internet Activities Board: Ethics and the Internet
- Code of Fair Information Practices

Summary

Test Your Skills

Table of Contents

Chapter 8: Physical Security Control

- Introduction
- Understanding the Physical Security Domain
  - Physical Security Threats
  - Providing Physical Security
- Summary
- Test Your Skills

Chapter 9: Operations Security

- Introduction
- Operations Security Principles
- Operations Security Process Controls
- Operations Security Controls in Action
  - Software Support
  - Configuration and Change Management
  - Backups
  - Media Controls
  - Documentation
  - Maintenance
  - Interdependencies
- Summary
- Test Your Skills

Chapter 10: Access Control Systems and Methodology

- Introduction
- Terms and Concepts
  - Identification
  - Authentication
  - Least Privilege (Need to Know)
  - Information Owner

Table of Contents

Discretionary Access Control
Access Control Lists
User Provisioning
Mandatory Access Control
Role-Based Access Control
Principles of Authentication
The Problems with Passwords
Multifactor Authentication
Biometrics
Single Sign-On
Kerberos
Federated Identities
Remote User Access and Authentication
Remote Access Dial-In User Service
Virtual Private Networks
Summary
Test Your Skills
Chapter 11: Cryptography
Introduction
Applying Cryptography to Information Systems
Basic Terms and Concepts
Strength of Cryptosystems
Cryptosystems Answer the Needs of Todays E-Commerce
The Role of Keys in Cryptosystems
Putting the Pieces to Work
Digesting Data
Digital Certificates
Examining Digital Cryptography

Table of Contents

Hashing Functions

Block Ciphers

Implementations of PPK Cryptography

Summary

Test Your Skills

Chapter 12: Telecommunications, Network, and Internet Security

Introduction

An Overview of Network and Telecommunications Security

Network Security in Context

The Open Systems Interconnection Reference Model

The Protocol Stack

The OSI Reference Model and TCP/IP

The OSI Model and Security

Data Network Types

Local Area Networks

Wide Area Networks

Internet

Intranet

Extranet

Protecting TCP/IP Networks

Basic Security Infrastructures

Routers

Firewalls

Intrusion Detection Systems

Intrusion Prevention Systems

Virtual Private Networks

IPSec

Table of Contents

Encapsulating Security Protocol
Security Association
Internet Security Association and Key Management Protocol
Security Policies
IPSec Key Management
Applied VPNs
Cloud Computing
Summary
Test Your Skills
Chapter 13: Software Development Security
Introduction
The Practice of Software Engineering
Software Development Life Cycles
Dont Bolt Security OnBuild It In
Catch Problems Sooner Rather Than Later
Requirements Gathering and Analysis
Systems Design and Detailed Design
Design Reviews
Development (Coding) Phase
Testing
Deployment
Security Training
Measuring the Secure Development Program
Open Software Assurance Maturity Model (OpenSAMM)
Building Security in Maturity Model (BSIMM)
Summary
Test Your Skills
Chapter 14: Securing the Future

Table of Contents

- Introduction
- Operation Eligible Receiver
- Carders, Account Takeover, and Identity Theft
  - Some Definitions
  - ZeuS Banking Trojan
  - Phishing and Spear Phishing
  - Other Trends in Internet (In)Security
  - The Year (Decade?) of the Breach
- The Rosy Future for InfoSec Specialists
- Summary
- Test Your Skills

Appendix A: Common Body of Knowledge

- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal Regulations, Investigations, and Compliance
- Physical (Environmental) Security

Appendix B: Security Policy and Standards Taxonomy

Appendix C: Sample Policies

- Sample Computer Acceptable Use Policy
  - 1.0.0 Acceptable Use Policy
- Sample Email Use Policy

Table of Contents

1.0.0 Email Use Policy

Sample Password Policy

1.0.0 Password Policy

Sample Wireless (WiFi) Use Policy

1.0.0 Wireless Communication Policy

Appendix D: HIPAA Security Rule Standards

HIPAA Security Standards

Administrative Procedures

Physical Safeguards

Technical Security Services

Technical Security Mechanisms

Index