



Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices



WILLIAM STALLINGS

Information Privacy Engineering and Privacy by Design

Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Dedication

Table of Contents

Preface

Part I: Overview

Chapter 1: Security and Cryptography Concepts

1.1 Cybersecurity, Information Security, and Network Security

Security Objectives

The Challenges of Information Security

1.2 Security Attacks

Passive Attacks

Active Attacks

1.3 Security Services

Authentication

Access Control

Data Confidentiality

Data Integrity

Table of Contents

Nonrepudiation

Availability Service

1.4 Security Mechanisms

1.5 Cryptographic Algorithms

Keyless Algorithms

Single-Key Algorithms

Two-Key Algorithms

1.6 Symmetric Encryption

1.7 Asymmetric Encryption

1.8 Cryptographic Hash Functions

1.9 Digital Signatures

1.10 Practical Considerations

Selection of Cryptographic Algorithms and Key Lengths

Implementation Considerations

Lightweight Cryptographic Algorithms

Post-Quantum Cryptographic Algorithms

1.11 Public-Key Infrastructure

Public-Key Certificates

PKI Architecture

1.12 Network Security

Communications Security

Device Security

1.13 Key Terms and Review Questions

Key Terms

Review Questions

1.14 References

Chapter 2: Information Privacy Concepts

2.1 Key Privacy Terminology

2.2 Privacy by Design

Privacy by Design Principles

Requirements and Policy Development

Table of Contents

Privacy Risk Assessment

Privacy and Security Control Selection

Privacy Program and Integration Plan

2.3 Privacy Engineering

Privacy Implementation

System Integration

Privacy Testing and Evaluation

Privacy Auditing and Incident Response

2.4 Privacy and Security

Areas of Overlap Between Security and Privacy

Trade-Offs Between Security and Privacy

2.5 Privacy Versus Utility

2.6 Usable Privacy

Users of Privacy Services and Functions

Usability and Utility

2.7 Key Terms and Review Questions

Key Terms

Review Questions

2.8 References

Part II: Privacy Requirements and Threats

Chapter 3: Information Privacy Requirements and Guidelines

3.1 Personally Identifiable Information and Personal Data

Sources of PII

Sensitivity of PII

3.2 Personal Information That Is Not PII

3.3 Fair Information Practice Principles

3.4 Privacy Regulations

European Union

U.S. Privacy Laws and Regulations

3.5 Privacy Standards

International Organization for Standardization (ISO)

Table of Contents

National Institute of Standards and Technology

3.6 Privacy Best Practices

Information Security Forum (ISF)

Cloud Security Alliance (CSA)

3.7 Key Terms and Review Questions

Key Terms

Review Questions

3.8 References

Chapter 4: Information Privacy Threats and Vulnerabilities

4.1 The Evolving Threat Environment

Overall Impact of Advances in Technology

Repurposing Collected Data

Means of Collection of PII

4.2 Privacy Threat Taxonomy

Information Collection

Information Processing

Information Dissemination

Invasions

4.3 NIST Threat Model

4.4 Threat Sources

4.5 Identifying Threats

4.6 Privacy Vulnerabilities

Vulnerability Categories

Location of Privacy Vulnerabilities

National Vulnerability Database and Common Vulnerability Scoring System

4.7 Key Terms and Review Questions

Key Terms

Review Questions

4.8 References

Part III: Technical Security Controls for Privacy

Chapter 5: System Access

Table of Contents

5.1 System Access Concepts

Privileges

System Access Functions

Privacy Considerations for System Access

5.2 Authorization

Privacy Authorization

5.3 User Authentication

Means of Authentication

Multifactor Authentication

A Model for Electronic User Authentication

5.4 Access Control

Subjects, Objects, and Access Rights

Access Control Policies

Discretionary Access Control

Role-Based Access Control

Attribute-Based Access Control

5.5 Identity and Access Management

IAM Architecture

Federated Identity Management

5.6 Key Terms and Review Questions

Key Terms

Review Questions

5.7 Reference

Chapter 6: Malicious Software and Intruders

6.1 Malware Protection Activities

Types of Malware

The Nature of the Malware Threat

Practical Malware Protection

6.2 Malware Protection Software

Capabilities of Malware Protection Software

Managing Malware Protection Software

6.3 Firewalls

Table of Contents

Firewall Characteristics

Types of Firewalls

Next-Generation Firewalls

DMZ Networks

The Modern IT Perimeter

6.4 Intrusion Detection

Basic Intrusion Detection Principles

Approaches to Intrusion Detection

Host-Based Intrusion Detection Techniques

Network-Based Intrusion Detection Systems

IDS Best Practices

6.5 Key Terms and Review Questions

Key Terms

Review Questions

6.6 References

Part IV: Privacy Enhancing Technologies

Chapter 7: Privacy in Databases

7.1 Basic Concepts

Personal Data Attributes

Types of Data Files

7.2 Re-Identification Attacks

Types of Attacks

Potential Attackers

Disclosure Risks

Applicability to Privacy Threats

7.3 De-Identification of Direct Identifiers

Anonymization

Pseudonymization

7.4 De-Identification of Quasi-Identifiers in Microdata Files

Privacy-Preserving Data Publishing

Disclosure Risk Versus Data Utility

PPDP Techniques

Table of Contents

7.5 K-Anonymity, L-Diversity, and T-Closeness

K-Anonymity

L-Diversity

T-Closeness

7.6 Summary Table Protection

Frequency Tables

Magnitude Tables

7.7 Privacy in Queryable Databases

Privacy Threats

Protecting Queryable Databases

7.8 Key Terms and Review Questions

Key Terms

Review Questions

7.9 References

Chapter 8: Online Privacy

8.1 The Online Ecosystem for Personal Data

8.2 Web Security and Privacy

Web Server Security and Privacy

Web Application Security and Privacy

Web Browser Security and Privacy

8.3 Mobile App Security

Mobile Ecosystem

Mobile Device Vulnerabilities

BYOD Policies

Mobile Application Vetting

Resources for Mobile Device Security

8.4 Online Privacy Threats

Web Application Privacy

Mobile App Privacy

8.5 Online Privacy Requirements

Online Privacy Principles

Online Privacy Framework

Table of Contents

- Simplified Consumer Choice
- Transparency of Data Practices

8.6 Privacy Notices

- Notice Requirements
- Notice Content
- Notice Structure
- Mobile App Privacy Notices
- Privacy Notice Design Space

8.7 Tracking

- Cookies
- Other Tracking Technologies
- Do Not Track

8.8 Key Terms and Review Questions

- Key Terms
- Review Questions

8.9 References

Chapter 9: Other PET Topics

9.1 Data Loss Prevention

- Data Classification and Identification
- Data States
- DLP for Email
- DLP Model

9.2 The Internet of Things

- Things on the Internet of Things
- Components of IoT-Enabled Things
- IoT and Cloud Context

9.3 IoT Security

- IoT Device Capabilities
- Security Challenges of the IoT Ecosystem
- IoT Security Objectives

9.4 IoT Privacy

- An IoT Model

Table of Contents

Privacy Engineering Objectives and Risks

Challenges for Organizations

9.5 Cloud Computing

Cloud Computing Elements

Threats for Cloud Service Users

9.6 Cloud Privacy

Data Collection

Storage

Sharing and Processing

Deletion

9.7 Key Terms and Review Questions

Key Terms

Review Questions

9.8 References

Part V: Information Privacy Management

Chapter 10: Information Privacy Governance and Management

10.1 Information Security Governance

Information Security Management System

Information Security Governance Concepts

Security Governance Components

Integration with Enterprise Architecture

Policies and Guidance

10.2 Information Privacy Governance

Information Privacy Roles

The Privacy Program Plan

10.3 Information Privacy Management

Key Areas of Privacy Management

Privacy Planning

Privacy Policy

10.4 OASIS Privacy Management Reference Model

Privacy Management Reference Model and Methodology (PMRM)

Privacy by Design Documentation for Software Engineers

Table of Contents

10.5 Key Terms and Review Questions

- Key Terms

- Review Questions

10.6 References

Chapter 11: Risk Management and Privacy Impact Assessment

11.1 Risk Assessment

- Risk Assessment Process

- Risk Assessment Challenges

- Quantitative Risk Assessment

- Qualitative Risk Assessment

11.2 Risk Management

- NIST Risk Management Framework

- ISO 27005: Information Security Risk Management

- Risk Evaluation

- Risk Treatment

11.3 Privacy Risk Assessment

- Privacy Impact

- Likelihood

- Assessing Privacy Risk

11.4 Privacy Impact Assessment

- Privacy Threshold Analysis

- Preparing for a PIA

- Identify PII Information Flows

- Identify Potential User Behavior

- Determine Relevant Privacy Safeguarding Requirements

- Assess Privacy Risk

- Determine Risk Treatment

- The PIA Report

- Implement Risk Treatment

- Review/Audit Implementation

- Examples

11.5 Key Terms and Review Questions

Table of Contents

Key Terms

Review Questions

11.6 References

Chapter 12: Privacy Awareness, Training, and Education

12.1 Information Privacy Awareness

Awareness Topics

Awareness Program Communication Materials

Awareness Program Evaluation

12.2 Privacy Training and Education

Cybersecurity Essentials

Role-Based Training

Education and Certification

12.3 Acceptable Use Policies

Information Security Acceptable Use Policy

PII Acceptable Use Policy

12.4 Key Terms and Review Questions

Key Terms

Review Questions

12.5 References

Chapter 13: Event Monitoring, Auditing, and Incident Response

13.1 Event Monitoring

Security Event Logging

Security Event Management

Event Logging Related to PII

13.2 Information Security Auditing

Data to Collect for Auditing

Internal and External Audits

Security Audit Controls

13.3 Information Privacy Auditing

Privacy Audit Checklist

Privacy Controls

13.4 Privacy Incident Management and Response

Table of Contents

Objectives of Privacy Incident Management

Privacy Incident Response Team

Preparing for Privacy Incident Response

Detection and Analysis

Containment, Eradication, and Recovery

Notification to Affected Individuals

Post-Incident Activity

13.5 Key Terms and Review Questions

Key Terms

Review Questions

13.6 References

Part VI: Legal and Regulatory Requirements

Chapter 14: The EU General Data Protection Regulation

14.1 Key Roles and Terms in the GDPR

14.2 Structure of the GDPR

14.3 GDPR Objectives and Scope

Objectives

Scope of the GDPR

14.4 GDPR Principles

Fairness

Lawful

Transparency

14.5 Restrictions on Certain Types of Personal Data

Children's Personal Data

Special Categories of Personal Data

14.6 Rights of the Data Subject

14.7 Controller, Processor, and Data Protection Officer

Data Protection by Design and Default

Records of Processing Activities

Security of Processing

Data Protection Officer

14.8 Data Protection Impact Assessment

Table of Contents

- Risk and High Risk
- Determining Whether a DPIA Is Needed
- DPIA Process
- GDPR Requirements
- Criteria for an Acceptable DPIA

14.9 Key Terms and Review Questions

- Key Terms
- Review Questions

14.10 References

Chapter 15: U.S. Privacy Laws

15.1 A Survey of Federal U.S. Privacy Laws

15.2 Health Insurance Portability and Accountability Act

- HIPAA Overview
- HIPAA Privacy Rule

15.3 Health Information Technology for Economic and Clinical Health Act

- Breach Notification
- Encryption of PHI
- Data Destruction

15.4 Childrens Online Privacy Protection Act

- General Provisions
- The COPPA Final Rule

15.5 California Consumer Privacy Act

- Basic Concepts
- Rights of Consumers
- Comparison with the GDPR

15.6 Key Terms and Review Questions

- Key Terms
- Review Questions

15.7 References

Index