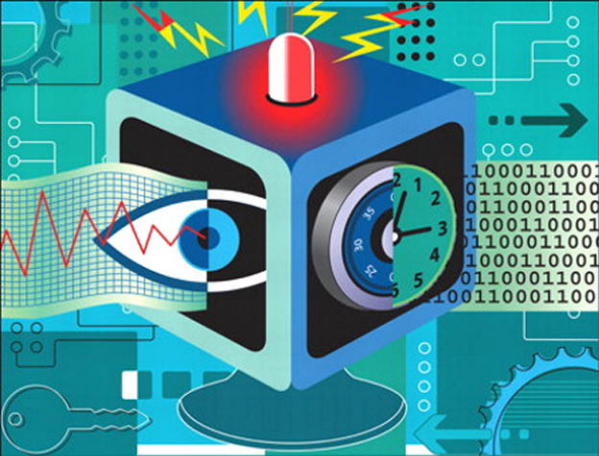




THE CRAFT OF SYSTEM SECURITY

Sean Smith
John Marchesini

The Craft of System Security

Craft of System Security, The

Table of Contents

Contents

Preface

Acknowledgments

Part I: History

1 Introduction

- 1.1 The Standard Rubric
- 1.2 The Matrix
- 1.3 Other Views
- 1.4 Safe States and the Access Control Matrix
- 1.5 Other Hard Questions
- 1.6 The Take-Home Message
- 1.7 Project Ideas

2 The Old Testament

- 2.1 The Basic Framework
- 2.2 Security Models
- 2.3 The Orange Book
- 2.4 INFOSEC, OPSEC, JOBSEC
- 2.5 The Take-Home Message
- 2.6 Project Ideas

3 Old Principles, New World

- 3.1 Solving the Wrong Problem?
- 3.2 Lack of Follow-Through?
- 3.3 Too Unwieldy?
- 3.4 Saltzer and Schroeder
- 3.5 Modern Relevance

Table of Contents

3.6 The Take-Home Message

3.7 Project Ideas

Part II: Security and the Modern Computing Landscape

4 OS Security

4.1 OS Background

4.2 OS Security Primitives and Principles

4.3 Real OSes: Everything but the Kitchen Sink

4.4 When the Foundation Cracks

4.5 Where Are We?

4.6 The Take-Home Message

4.7 Project Ideas

5 Network Security

5.1 Basic Framework

5.2 Protocols

5.3 The Network as a Battlefield

5.4 The Brave New World

5.5 The Take-Home Message

5.6 Project Ideas

6 Implementation Security

6.1 Buffer Overflow

6.2 Argument Validation and Other Mishaps

6.3 TOCTOU

6.4 Malware

6.5 Programming Language Security

6.6 Security in the Development Lifecycle

6.7 The Take-Home Message

6.8 Project Ideas

Part III: Building Blocks for Secure Systems

Table of Contents

7 Using Cryptography

- 7.1 Framework and Terminology
- 7.2 Randomness
- 7.3 Symmetric Cryptography
- 7.4 Applications of Symmetric Cryptography
- 7.5 Public-Key Cryptography
- 7.6 Hash Functions
- 7.7 Practical Issues: Public Key
- 7.8 Past and Future
- 7.9 The Take-Home Message
- 7.10 Project Ideas

8 Subverting Cryptography

- 8.1 Breaking Symmetric Key without Brute Force
- 8.2 Breaking Symmetric Key with Brute Force
- 8.3 Breaking Public Key without Factoring
- 8.4 Breaking Cryptography via the Real World
- 8.5 The Potential of Efficiently Factoring Moduli
- 8.6 The Take-Home Message
- 8.7 Project Ideas

9 Authentication

- 9.1 Basic Framework
- 9.2 Authenticating Humans
- 9.3 Human Factors
- 9.4 From the Machines Point of View
- 9.5 Advanced Approaches
- 9.6 Case Studies
- 9.7 Broader Issues
- 9.8 The Take-Home Message
- 9.9 Project Ideas

10 Public Key Infrastructure

Table of Contents

- 10.1 Basic Definitions
- 10.2 Basic Structure
- 10.3 Complexity Arrives
- 10.4 Multiple CAs
- 10.5 Revocation
- 10.6 The X.509 World
- 10.7 Dissent
- 10.8 Ongoing Trouble
- 10.9 The Take-Home Message
- 10.10 Project Ideas

11 Standards, Compliance, and Testing

- 11.1 Standards
- 11.2 Policy Compliance
- 11.3 Testing
- 11.4 The Take-Home Message
- 11.5 Project Ideas

Part IV: Applications

12 The Web and Security

- 12.1 Basic Structure
- 12.2 Security Techniques
- 12.3 Privacy Issues
- 12.4 Web Services
- 12.5 The Take-Home Message
- 12.6 Project Ideas

13 Office Tools and Security

- 13.1 Word
- 13.2 Lotus 1-2-3
- 13.3 PDF
- 13.4 Cut-and-Paste
- 13.5 PKI and Office Tools

Table of Contents

13.6 Mental Models

13.7 The Take-Home Message

13.8 Project Ideas

14 Money, Time, Property

14.1 Money

14.2 Time

14.3 Property

14.4 The Take-Home Message

14.5 Project Ideas

Part V: Emerging Tools

15 Formal Methods and Security

15.1 Specification

15.2 Logics

15.3 Cranking the Handle

15.4 Case Studies

15.5 Spinning Your Bank Account

15.6 Limits

15.7 The Take-Home Message

15.8 Project Ideas

16 Hardware-Based Security

16.1 Data Remanence

16.2 Attacks and Defenses

16.3 Tools

16.4 Alternative Architectures

16.5 Coming Trends

16.6 The Take-Home Message

16.7 Project Ideas

17 In Search of the Evil Bit

17.1 The AI Toolbox

Table of Contents

- 17.2 Application Taxonomy
- 17.3 Case Study
- 17.4 Making it Real
- 17.5 The Take-Home Message
- 17.6 Project Ideas

18 Human Issues

- 18.1 The Last Mile
- 18.2 Design Principles
- 18.3 Other Human-Space Issues
- 18.4 Trust
- 18.5 The Take-Home Message
- 18.6 Project Ideas

The Take-Home Lesson

A: Exiled Theory

- A.1 Relations, Orders, and Lattices
- A.2 Functions
- A.3 Computability Theory
- A.4 Frameworks
- A.5 Quantum Physics and Quantum Computation

Bibliography

Index