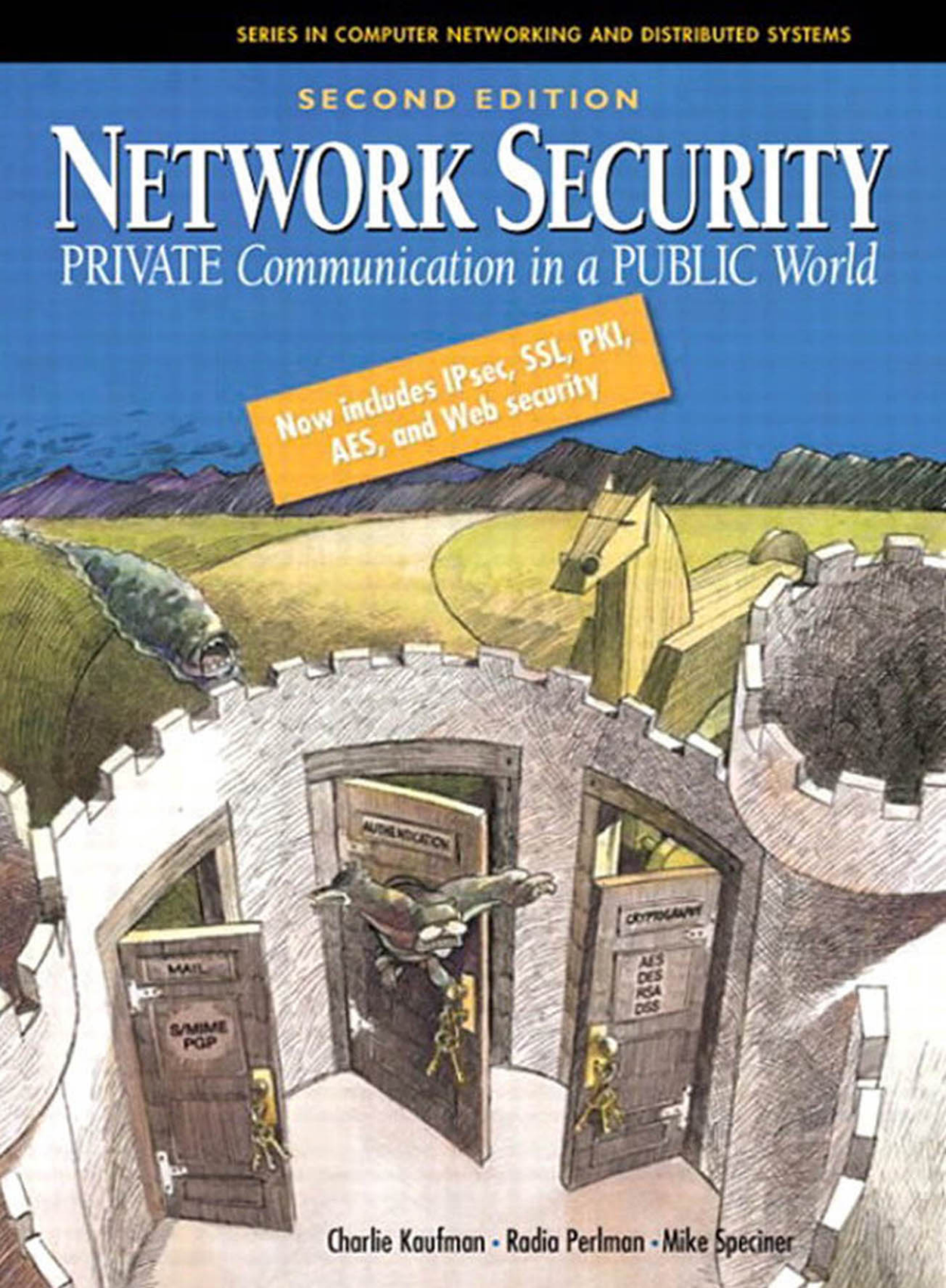
SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS

SECOND EDITION

NETWORK SECURITY

PRIVATE *Communication in a* PUBLIC *World*

Now includes IPsec, SSL, PKI, AES, and Web security



Charlie Kaufman • Radia Perlman • Mike Speciner

NETWORK SECURITY

PRIVATE Communication in a PUBLIC World

ISBN 0-13-046019-2

Network Security: Private Communications in a Public World

Table of Contents

Cover
Half Title
Title Page
Copyright Page
Contents
Acknowledgments
CHAPTER 1 Introduction
- 1.1 Roadmap to the Book
- 1.2 What Type of Book Is This?
- 1.3 Terminology
- 1.4 Notation
- 1.5 Primer on Networking
  - 1.5.1 OSI Reference Model
  - 1.5.2 IP, UDP, and TCP
  - 1.5.3 Directory Service
  - 1.5.4 Replicated Services
  - 1.5.5 Packet Switching
  - 1.5.6 Network Components
  - 1.5.7 Destinations: Ultimate and Next-Hop
  - 1.5.8 Address Structure
- 1.6 Active vs. Passive Attacks

Table of Contents

1.7 Layers and Cryptography

1.8 Authorization

1.9 Tempest

1.10 Key Escrow for Law Enforcement

1.11 Key Escrow for Careless Users

1.12 Viruses, Worms, Trojan Horses

1.12.1 Where Do They Come From?

1.12.2 Spreading Pests from Machine to Machine

1.12.3 Virus Checkers

1.12.4 What Can We Do Today?

1.12.5 Wish List for the Future

1.13 The Multi-level Model of Security

1.13.1 Mandatory (Nondiscretionary) Access Controls

1.13.2 Levels of Security

1.13.3 Mandatory Access Control Rules

1.13.4 Covert Channels

1.13.5 The Orange Book

1.13.6 Successors to the Orange Book

1.14 Legal Issues

1.14.1 Patents

1.14.2 Export Controls

CRYPTOGRAPHY

CHAPTER 2 Introduction to Cryptography

2.1 What Is Cryptography?

2.2 Breaking an Encryption Scheme

2.3 Types of Cryptographic Functions

2.4 Secret Key Cryptography

Table of Contents

2.5 Public Key Cryptography

2.6 Hash Algorithms

2.7 Homework

CHAPTER 3 Secret Key Cryptography

3.1 Introduction

3.2 Generic Block Encryption

3.3 Data Encryption Standard (DES)

3.4 International Data Encryption Algorithm (IDEA)

3.5 Advanced Encryption Standard (AES)

3.6 RC4

3.7 Homework

CHAPTER 4 Modes of Operation

4.1 Introduction

4.2 Encrypting a Large Message

4.3 Generating MACs

4.4 Multiple Encryption DES

4.5 Homework

CHAPTER 5 Hashes and Message Digests

5.1 Introduction

5.2 Nifty Things to Do with a Hash

5.3 MD2

5.4 MD4

5.5 MD5

5.6 SHA-1

5.7 HMAC

5.8 Homework

CHAPTER 6 Public Key Algorithms

6.1 Introduction

Table of Contents

6.2 Modular Arithmetic

6.3 RSA

6.4 Diffie-Hellman

6.5 Digital Signature Standard (DSS)

6.6 How Secure Are RSA and Diffie-Hellman?

6.7 Elliptic Curve Cryptography (ECC)

6.8 Zero Knowledge Proof Systems

6.9 Homework Problems

CHAPTER 7 Number Theory

7.1 Introduction

7.2 Modular Arithmetic

7.3 Primes

7.4 Euclid's Algorithm

7.5 Chinese Remainder Theorem

7.6 Z[sub(n)]*

7.7 Euler's Totient Function

7.8 Euler's Theorem

7.9 Homework Problems

CHAPTER 8 Math with AES and Elliptic Curves

8.1 Introduction

8.2 Notation

8.3 Groups

8.4 Fields

8.5 Mathematics of Rijndael

8.6 Elliptic Curve Cryptography

8.7 Homework

AUTHENTICATION

CHAPTER 9 Overview of Authentication Systems

Table of Contents

9.1 Password-Based Authentication
9.2 Address-Based Authentication
9.3 Cryptographic Authentication Protocols
9.4 Who Is Being Authenticated?
9.5 Passwords as Cryptographic Keys
9.6 Eavesdropping and Server Database Reading
9.7 Trusted Intermediaries
9.8 Session Key Establishment
9.9 Delegation
9.10 Homework

CHAPTER 10 Authentication of People

10.1 Passwords
10.2 On-Line Password Guessing
10.3 Off-Line Password Guessing
10.4 How Big Should a Secret Be?
10.5 Eavesdropping
10.6 Passwords and Careless Users
10.7 Initial Password Distribution
10.8 Authentication Tokens
10.9 Physical Access
10.10 Biometrics
10.11 Homework

CHAPTER 11 Security Handshake Pitfalls

11.1 Login Only
11.2 Mutual Authentication
11.3 Integrity/Encryption for Data
11.4 Mediated Authentication (with KDC)
11.5 Nonce Types

Table of Contents

11.6 Picking Random Numbers

11.7 Performance Considerations

11.8 Authentication Protocol Checklist

11.9 Homework

CHAPTER 12 Strong Password Protocols

12.1 Introduction

12.2 Lamport's Hash

12.3 Strong Password Protocols

12.4 Strong Password Credentials Download Protocols

12.5 Homework

STANDARDS

CHAPTER 13 Kerberos V4

13.1 Introduction

13.2 Tickets and Ticket-Granting Tickets

13.3 Configuration

13.4 Logging Into the Network

13.5 Replicated KDCs

13.6 Realms

13.7 Interrealm Authentication

13.8 Key Version Numbers

13.9 Encryption for Privacy and Integrity

13.10 Encryption for Integrity Only

13.11 Network Layer Addresses in Tickets

13.12 Message Formats

13.13 Homework

CHAPTER 14 Kerberos V5

14.1 ASN.1

14.2 Names

Table of Contents

14.3 Delegation of Rights
14.4 Ticket Lifetimes
14.5 Key Versions
14.6 Making Master Keys in Different Realms Different
14.7 Optimizations
14.8 Cryptographic Algorithms
14.9 Hierarchy of Realms
14.10 Evading Password-Guessing Attacks
14.11 Key Inside Authenticator
14.12 Double TGT Authentication
14.13 PKINITPublic Keys for Users
14.14 KDC Database
14.15 Kerberos V5 Messages
14.16 Homework

CHAPTER 15 PKI (Public Key Infrastructure)

15.1 Introduction
15.2 Some Terminology
15.3 PKI Trust Models
15.4 Revocation
15.5 Directories and PKI
15.6 PKIX and X.509
15.7 X.509 and PKIX Certificates
15.8 Authorization Futures
15.9 Homework

CHAPTER 16 Real-time Communication Security

16.1 What Layer?
16.2 Session Key Establishment
16.3 Perfect Forward Secrecy

Table of Contents

16.4 PFS-Foilage
16.5 Denial-of-Service/Clogging Protection
16.6 Endpoint Identifier Hiding
16.7 Live Partner Reassurance
16.8 Arranging for Parallel Computation
16.9 Session Resumption
16.10 Plausible Deniability
16.11 Data Stream Protection
16.12 Negotiating Crypto Parameters
16.13 Easy Homework
16.14 Homework

CHAPTER 17 IPsec: AH and ESP

17.1 Overview of IPsec
17.2 IP and IPv6
17.3 AH (Authentication Header)
17.4 ESP (Encapsulating Security Payload)
17.5 So, Do We Need AH?
17.6 Comparison of Encodings
17.7 Easy Homework
17.8 Homework

CHAPTER 18 IPsec: IKE

18.1 Photuris
18.2 SKIP
18.3 History of IKE
18.4 IKE Phases
18.5 Phase 1 IKE
18.6 Phase-2 IKE: Setting up IPsec SAs
18.7 ISAKMP/IKE Encoding

Table of Contents

18.8 Homework

CHAPTER 19 SSL/TLS

19.1 Introduction

19.2 Using TCP

19.3 Quick History

19.4 SSL/TLS Basic Protocol

19.5 Session Resumption

19.6 Computing the Keys

19.7 Client Authentication

19.8 PKI as Deployed by SSL

19.9 Version Numbers

19.10 Negotiating Cipher Suites

19.11 Negotiating Compression Method

19.12 Attacks Fixed in v3

19.13 Exportability

19.14 Encoding

19.15 Further Reading

19.16 Easy Homework

19.17 Homework

ELECTRONIC MAIL

CHAPTER 20 Electronic Mail Security

20.1 Distribution Lists

20.2 Store and Forward

20.3 Security Services for Electronic Mail

20.4 Establishing Keys

20.5 Privacy

20.6 Authentication of the Source

20.7 Message Integrity

Table of Contents

20.8 Non-Repudiation
20.9 Proof of Submission
20.10 Proof of Delivery
20.11 Message Flow Confidentiality
20.12 Anonymity
20.13 Containment
20.14 Annoying Text Format Issues
20.15 Names and Addresses
20.16 Verifying When a Message Was Really Sent
20.17 Homework

CHAPTER 21 PEM & S/MIME

21.1 Introduction
21.2 Structure of a PEM Message
21.3 Establishing Keys
21.4 Some PEM History
21.5 PEM Certificate Hierarchy
21.6 Certificate Revocation Lists (CRLs)
21.7 Reformatting Data to Get Through Mailers
21.8 General Structure of a PEM Message
21.9 Encryption
21.10 Source Authentication and Integrity Protection
21.11 Multiple Recipients
21.12 Bracketing PEM Messages
21.13 Forwarding and Enclosures
21.14 Unprotected Information
21.15 Message Formats
21.16 DES-CBC as MIC Doesn't Work
21.17 Differences in S/MIME

Table of Contents

21.18 S/MIME Certificate Hierarchy

21.19 Homework

CHAPTER 22 PGP (Pretty Good Privacy)

22.1 Introduction

22.2 Overview

22.3 Key Distribution

22.4 Efficient Encoding

22.5 Certificate and Key Revocation

22.6 Signature Types

22.7 Your Private Key

22.8 Key Rings

22.9 Anomalies

22.10 Object Formats

LEFTOVERS

CHAPTER 23 Firewalls

23.1 Packet Filters

23.2 Application Level Gateway

23.3 Encrypted Tunnels

23.4 Comparisons

23.5 Why Firewalls Don't Work

23.6 Denial-of-Service Attacks

23.7 Should Firewalls Go Away?

CHAPTER 24 More Security Systems

24.1 NetWare V3

24.2 NetWare V4

24.3 KryptoKnight

24.4 DASS/SPX

24.5 Lotus Notes Security

Table of Contents

24.6 DCE Security

24.7 Microsoft Windows Security

24.8 Network Denial of Service

24.9 Clipper

24.10 Homework

CHAPTER 25 Web Issues

25.1 Introduction

25.2 URLs/URIs

25.3 HTTP

25.4 HTTP Digest Authentication

25.5 Cookies

25.6 Other Web Security Problems

25.7 Homework

CHAPTER 26 Folklore

26.1 Perfect Forward Secrecy

26.2 Change Keys Periodically

26.3 Multiplexing Flows over a Single SA

26.4 Use Different Keys in the Two Directions

26.5 Use Different Secret Keys for Encryption vs. Integrity Protection

26.6 Use Different Keys for Different Purposes

26.7 Use Different Keys for Signing vs. Encryption

26.8 Have Both Sides Contribute to the Master Key

26.9 Don't Let One Side Determine the Key

26.10 Hash in a Constant When Hashing a Password

26.11 HMAC Rather than Simple MD

26.12 Key Expansion

26.13 Randomly Chosen IVs

26.14 Use of Nonces in Protocols

Table of Contents

26.15 Don't Let Encrypted Data Begin with a Constant
26.16 Don't Let Encrypted Data Begin with a Predictable Value
26.17 Compress Data Before Encrypting It
26.18 Don't Do Encryption Only
26.19 Avoiding Weak Keys
26.20 Minimal vs. Redundant Designs
26.21 Overestimate the Size of Key
26.22 Hardware Random Number Generators
26.23 Timing Attacks
26.24 Put Checksums at the End of Data
26.25 Forward Compatibility
26.26 Negotiating Parameters
26.27 Homework

Bibliography

Glossary

A
B
C
D
E
F
G
H
I
K
L
M

Table of Contents

N
O
P
R
S
T
U
V
W
X
Y
Z
Index