SECURITY

IN FIXED AND WIRELESS NETWORKS

an introduction to securing data communications

Günter Schäfer

WILEY

Security in Fixed and Wireless Networks

An Introduction to Securing Data Communications

Günter Schäfer
Technische Universität, Berlin, Germany

Translated by Hedwig Jourdan von Schmoeger, London, UK

WILEY

First published under the title Netzsicherheit. Algorithmische Grundlagen und Protokolle
ISBN: 3-89864-212-7 by dpunkt. verlag GmbH

Other Wiley Editorial Offices

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons (Canada) Ltd, 22 Worcester Road, Etobicoke, Rexdale, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0-470-86370-6

Typeset from pdf files supplied by the author.
Printed and bound in Great Britain by Antony Rowe, Chippenham, Wiltshire.
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Security in Fixed and Wireless Networks

About the Author

Dr.–Ing. Günter Schäfer studied computer science at the Universität Karlsruhe, Germany, from 1989 to 1994. After his studies he continued there as a member of the scientific staff at the Institute of Telematics.
He received his doctorate on the topic Efficient Authentication and Key Management in High-Performance Networks in October 1998. In February 1999 Dr Schäfer took a postdoctoral position at the Ecole Nationale Supérieure des Télécommunications in Paris, France, where he focused on network security and access network performance of third-generation mobile communication networks.

Since August 2000, Dr Schäfer has been at the Technische Universität Berlin, Germany, where he is involved in research and lectures on the subject of telecommunications networks. His main subject areas are network security, mobile communications, and active network technologies.

Günter Schäfer is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Gesellschaft für Informatik (German Computer Science Society).

Acknowledgements

This book has evolved during my time as a scientific assistant in the department of telecommunication networks at the Technische Universität Berlin, Germany. It is based on my lecture, Network Security, which I have been presenting at the University since the winter semester of 2000/2001.

I therefore particularly want to express my warm gratitude to the head of this department, Professor Adam Wolisz, for the wonderful opportunities he has given me for my work. He has supported my plans to write a textbook on network security from the very beginning.

Dipl.-Ing. Mr Andreas Hess offered to read and edit the entire first draft of my text. I am sincerely grateful to him for his fast turnaround times and numerous helpful suggestions for changes and improvements.

Mrs Hedwig Jourdan von Schmoeger translated the German version of the book into English. She not only had a good grasp of the technical content but also had a knack for dealing with my often rather long German sentences. I want to thank her for the very good working relationship we had.

This gratitude also extends to the editorial staff of dpunkt.verlag and John Wiley & Sons, who were so helpful with both the German and English versions of the book. Their constant support and guidance made my task much easier. I also appreciate the helpful input from the various reviewers who provided useful and constructive comments.

Lastly, I want to thank the students who attended my lectures for their numerous questions and suggestions that gave me many ideas for how to structure this book. The responsibility for any errors that still might appear in this book despite all the help that was available, of course, lies with me. I will, therefore, continue to appreciate any comments or suggestions regarding the content of this book.

Berlin, December 2003

Günter Schäfer
(securitybook@guenterschaefer.de)

This book has an accompying website that contains suport material for lecturers as well as sample chapters.

Please visit http://www.guenterschaefer.de/SecurityBook

Contents

I Foundations of Data Security Technology

1 Introduction 3
1.1 Content and Structure of this Book 4
1.2 Threats and Security Goals 6
1.3 Network Security Analysis 9
1.4 Information Security Measures 12
1.5 Important Terms Relating to Communication Security 14

2 Fundamentals of Cryptology 17
2.1 Cryptology, Cryptography and Cryptanalysis 17
2.2 Classification of Cryptographic Algorithms 18
2.3 Cryptanalysis 19
2.4 Estimating the Effort Needed for Cryptographic Analyses 21
2.5 Characteristics and Classification of Encryption Algorithms 23
2.6 Key Management 25
2.7 Summary 27
2.8 Supplemental Reading 28
2.9 Questions 29

3 Symmetric Cryptography 31
3.1 Encryption Modes of Block Ciphers 31
3.2 Data Encryption Standard 37
3.3 Advanced Encryption Standard 43
3.4 RC4 Algorithm 46
3.5 Summary 50
3.6 Supplemental Reading 51
3.7 Questions 52

4 Asymmetric Cryptography 53
4.1 Basic Idea of Asymmetric Cryptography 53
4.2 Mathematical Principles 56
4.3 The RSA Algorithm 65
4.4 The Problem of the Discrete Logarithm 67

4.5	The Diffie–Hellman Key Exchange Algorithm	71
4.6	The ElGamal Algorithm	73
4.7	Security of Asymmetric Cryptographic Schemes	76
4.8	Summary	78
4.9	Supplemental Reading	79
4.10	Exercises	80
5	**Cryptographic Check Values**	**83**
5.1	Requirements and Classification	83
5.2	Modification Detection Codes	85
5.3	Message Authentication Codes	94
5.4	Hybrid Schemes	97
5.5	Summary	98
5.6	Supplemental Reading	99
5.7	Questions	100
6	**Random Number Generation**	**101**
6.1	Random Numbers and Pseudo-Random Numbers	101
6.2	Cryptographically Secure Random Numbers	102
6.3	Statistical Tests for Random Numbers	104
6.4	Generation of Random Numbers	105
6.5	Generating Secure Pseudo-Random Numbers	106
6.6	Summary	109
6.7	Supplemental Reading	109
6.8	Questions	110
7	**Cryptographic Protocols**	**111**
7.1	Properties and Notation of Cryptographic Protocols	111
7.2	Data Origin and Entity Authentication	113
7.3	Needham–Schroeder Protocol	117
7.4	Kerberos	121
7.5	International Standard X.509	127
7.6	Security of Negotiated Session Keys	131
7.7	Formal Validation of Cryptographic Protocols	133
7.8	Summary	143
7.9	Supplemental Reading	144
7.10	Questions	144
8	**Access Control**	**147**
8.1	Definition of Terms and Concepts	147
8.2	Security Labels	149
8.3	Specification of Access Control Policies	150
8.4	Categories of Access Control Mechanisms	151

8.5 Summary 153
8.6 Supplemental Reading 154
8.7 Questions 154

II Network Security

9 Integration of Security Services 159
9.1 Motivation 159
9.2 A Pragmatic Model 161
9.3 General Considerations for Placement of Security Services .. 163
9.4 Integration in Lower Protocol Layers vs Applications 166
9.5 Integration into End Systems or Intermediate Systems 167
9.6 Summary 169
9.7 Supplemental Reading 169
9.8 Questions 169

10 Link Layer Security Protocols 171
10.1 Securing a Local Network Infrastructure Using IEEE 802.1x . 172
10.2 Point-to-Point Protocol 174
10.3 Point-to-Point Tunnelling Protocol 183
10.4 Virtual Private Networks 188
10.5 Summary 190
10.6 Supplemental Reading 192
10.7 Questions 193

11 IPSec Security Architecture 195
11.1 Short Introduction to the Internet Protocol Suite 195
11.2 Overview of IPSec Architecture 198
11.3 Use of Transport and Tunnel Mode 206
11.4 IPSec Protocol Processing 209
11.5 The ESP Protocol 212
11.6 The AH Protocol 218
11.7 The ISAKMP Protocol 223
11.8 Internet Key Exchange 231
11.9 Other Aspects of IPSec 237
11.10 Summary 238
11.11 Supplemental Reading 239
11.12 Questions 241

12 Transport Layer Security Protocols 243
12.1 Secure Socket Layer (SSL) 243
12.2 Transport Layer Security (TLS) 256
12.3 Secure Shell (SSH) 257

12.4 Summary ... 266
12.5 Supplemental Reading ... 267
12.6 Questions ... 267

13 Internet Firewalls ... 269
13.1 Tasks and Basic Principles of Firewalls ... 269
13.2 Firewall-Relevant Internet Services and Protocols ... 271
13.3 Terminology and Building Blocks ... 273
13.4 Firewall Architectures ... 275
13.5 Packet Filtering ... 279
13.6 Bastion Hosts and Proxy Servers ... 284
13.7 Summary ... 287
13.8 Supplemental Reading ... 287
13.9 Questions ... 288

III Secure Wireless and Mobile Communications

14 Security Aspects of Mobile Communication ... 291
14.1 Threats in Mobile Communication Networks ... 291
14.2 Protecting Location Confidentiality ... 292
14.3 Summary ... 297
14.4 Supplemental Reading ... 297
14.5 Questions ... 297

15 Security in Wireless Local Area Networks ... 299
15.1 The IEEE 802.11 Standard for Wireless Local Area Networks 299
15.2 Entity Authentication ... 301
15.3 Wired Equivalent Privacy ... 303
15.4 Summary ... 310
15.5 Supplemental Reading ... 311
15.6 Questions ... 312

16 Security in Mobile Wide-Area Networks ... 315
16.1 GSM ... 315
16.2 UMTS Release '99 ... 322
16.3 Summary ... 329
16.4 Supplemental Reading ... 329
16.5 Questions ... 330

17 Security of Mobile Internet Communication ... 333
17.1 Mobile IP ... 333
17.2 Security Aspects of Mobile IP ... 340
17.3 Integrated AAA/Mobile IP Authentication ... 342

17.4 Summary 351
17.5 Supplemental Reading 353
17.6 Questions 354

Bibliography 357

Abbreviations 373

Index 379

Part I

Foundations of Data Security Technology

1 Introduction

It is now a well-known fact that, despite all the benefits, the digital revolution with its omnipresent networking of information systems also involves some risks. This book looks at a specific category of risks and, in particular, the measures that can be taken to minimise them. The category of risks discussed has evolved as a result of eavesdropping and the manipulation of data transmitted in communication networks and the vulnerability of the communication infrastructure itself.

Protecting transmitted data

Mankind very early on recognised the need to protect information that was being transferred or stored, and so the desire to protect information from unauthorised access is probably as old as writing itself. For example, reliable early records on protective measures describe a technique used by the Spartans around 400 BC. The technique entailed writing messages on a leather strip that was wrapped around a stick of a certain diameter. Before the message was delivered, the leather strip was removed from the stick, and a potential attacker who did not have a stick with the same diameter (because he did not know the diameter or anything about the technique) could not read the message. In a sense this was an implementation of the first 'analogue' encryption.

First substitution ciphers

In the fourth century BC, the Greek Polybius developed a table of bilateral substitution that defined how to encode characters into pairs of symbols and their corresponding reinstatement, thereby specifying the first 'digital' encryption method. Of the Romans we know that they often protected their tactical communication by using simple monoalphabetic substitution methods. The best known one was probably the 'Caesar cipher', named after its creator Julius Caesar, in which each character of the alphabet is shifted upwards by three characters. Thus, 'A' becomes 'D', 'B' becomes 'E', etc.

Origins of cryptanalysis

The Arabs were the first people to develop a basic understanding of the two fundamental principles of *substitution*, i.e., pure character substitution, and *transposition*, i.e., changing the se-

quence of the characters of a text. When they evaluated a method they also considered how a potential attacker might analyse it. They were therefore aware of the significance of relative letter frequency in a language for the analysis of substitution ciphers, because it gave some insight into substitution rules. By the beginning of the fifteenth century, the Arabic encyclopaedia 'Subh al-a'sha' already contained an impressive treatment and analysis of cryptographic methods.

In Europe, cryptology originated during the Middle Ages in the papal and Italian city states. The first encryption algorithms merely involved vowel substitution, and therefore offered at least some rudimentary protection from totally ignorant attackers who may not have come up with the idea of trying out all the different possible vowel substitutions.

Protection of infrastructure

Not wanting to turn the entire development of cryptology into a scientific discipline at this juncture, we can deduce from the developments mentioned that special importance has always been given to protecting information. However, a second category of risks is increasingly becoming a major priority in the age of omnipresent communication networks. These risks actually affect communication infrastructures rather than the data being transmitted. With the development and expansion of increasingly complex networks, and the growing importance of these networks not only to the economic but also to the social development of the modern information society, there is also a greater demand for ways to secure communication infrastructures from deliberate manipulation. For economic operation it is important to ensure that the services provided by communication networks are available and functioning properly and that the use of these services can be billed correctly and in a way that everyone can understand.

1.1 Content and Structure of this Book

In this book equal treatment is given to the two task areas in network security mentioned – *security of transmitted data* and *security of the communication infrastructure*. We start by introducing central terms and concepts and providing an overview of the measures available for information security.

Part 1 of the book deals with fundamental principles

Building on this introductory information, the rest of the chapters in Part 1 deal with the *fundamental principles of data security technology*. Chapter 2 uses basic concepts to introduce cryptology. Chapter 3 covers the use and functioning of symmetric cipher-

ing schemes, whereas Chapter 4 is devoted to asymmetric cryptographic algorithms. Chapter 5 introduces cryptographic check values for the detection of message manipulation. Generating secure, non-predictable random numbers is the subject of Chapter 6. In a sense, the algorithms in these four chapters constitute the *basic primitives* of data security technology upon which the cryptographic protection mechanisms of network security are based. Chapter 7 discusses cryptographic protocols and introduces the authentication and key exchange protocols that are central to network security. Part 1 concludes with Chapter 8, which provides an introduction to the principles of access control.

Part 2 introduces architectures and protocols for network security

Part 2 of this book focuses on the architectures and protocols of *network security*. It starts with Chapter 9, which examines general issues relating to the integration of security services in communication architectures. Chapter 10 discusses security protocols of the data link layer, Chapter 11 examines the security architecture for the Internet protocol *IPSec*, and Chapter 12 describes the security protocols for the transport layer. Part 2 concludes with Chapter 13, which introduces *Internet firewalls* for realising subnetwork-related access control.

Part 3 is devoted to wireless and mobile communication

The last part of the book, Part 3, presents the field of *secure wireless or mobile communication*. Chapter 14 differentiates the additional security aspects that arise in mobile communication compared with conventional fixed networks, and presents approaches of a more conceptual nature for maintaining the confidentiality of the current location area of mobile devices. The other chapters in this part examine concrete examples of systems. Chapter 15 deals with the security functions and weaknesses of the IEEE 802.11 standard for wireless local networks. Chapter 16 introduces the security functions for the two European standards for mobile wide-area networks *GSM* and *UMTS* and concluding Chapter 17 covers the fundamental aspects of secure mobile Internet communication based on the *Mobile IP* approach.

The field of network security is currently marked by a major dynamic

Before our attentive and inquisitive readers get too involved in the further content of this book, they should be made aware that the field of network security has developed into a very active field during the last few years. Consequently, extensive improvements are constantly being made to existing security protocols and new protocols are being developed and introduced. Doing justice to the speed of this development in a textbook therefore becomes a very difficult if not impossible undertaking. We therefore ask for the reader's understanding if a detail or two has already been

resolved in a way that deviates from our interpretation in a particular chapter or totally new protocols have established themselves in the meantime and are not dealt with in this book. It is precisely because of the rapid developments in this field that the priority of this book is to provide the reader with a fundamental understanding of the central principles presented and to describe them on the basis of concrete and relevant sample protocols.

1.2 Threats and Security Goals

The terms *threat* and *security goal* play an important role in assessing the risks in communication networks. Therefore, they will first be defined in general terms.

Definition 1.1 *A* **threat** *in a communication network is a potential event or series of events that could result in the violation of one or more security goals. The actual implementation of a threat is called an* **attack**.

Examples of concrete threats

Definition 1.1 given above is kept quite abstract and refers to the term security goal defined below. The following examples clarify the types of threats that exist:

- a 'hacker' intruding into the computer of a company;
- someone reading someone else's transmitted e-mails;
- a person altering sensitive data in a financial accounting system;
- a hacker temporarily shutting down a web site;
- somebody using or ordering services and goods in someone else's name.

Examples of security goals

The term *security goal* is another concept that is easier to explain with examples because at first glance security goals can vary considerably depending on the respective application scenario:

- Banks:
  - protection from deliberate or unintentional modification of transactions;
  - reliable and non-manipulable identification of customers;