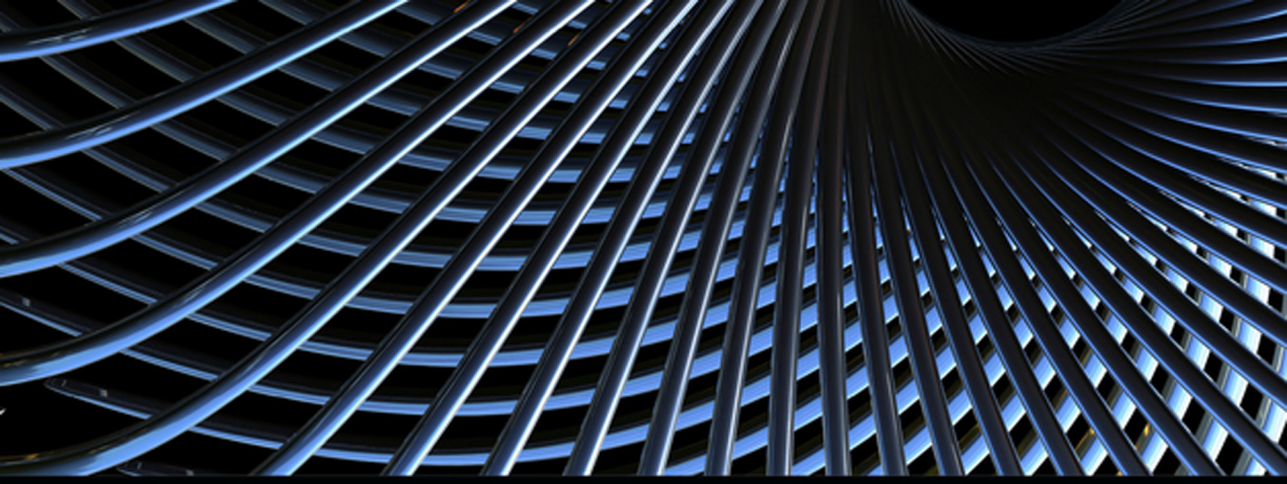

2nd Edition

Security in Fixed and Wireless Networks

Guenter Schaefer
Michael Rossberg

WILEY

Security in Fixed and Wireless Networks (2nd Edition)

Security in Fixed and Wireless Networks (2nd Edition)

Guenter Schaefer and Michael Rossberg
Technische Universitaet Ilmenau, Germany

Translation by HE Translations, Leicester, UK
www.HETranslations.uk

WILEY

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

Library of Congress Cataloging-in-Publication Data

Schaefer, Guenter (Telecommunications engineer), author.
[Netzsicherheit, Algorithmische Grundlagen und Protokolle. English]
Security in fixed and wireless networks / Dr Guenter Schaefer, Technische Universitaet Ilmenau, Michael Rossberg, Technische Universitaet Ilmenau.
pages cm
Includes bibliographical references and index.
ISBN 978-1-119-04074-3 (cloth : alk. paper) 1. Computer networks–Security measures. 2. Wireless communication systems–Security measures. 3. Computer security. I. Rossberg, Michael, author. II. Title.
TK5105.59.S3313 2003
005.8—dc23
2015034626

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

Set in 10/13pt, NewCenturySchlbkLTStd by SPi Global, Chennai, India.

1 2016

Contents

About the authors

Guenter Schaefer studied computer science at Universitaet Karlsruhe, Germany, from 1989 to 1994. Between 1994 and 1999 he was a researcher at the Institute of Telematics, Universitaet Karlsruhe. After obtaining his PhD degree (1998) he worked at Ecole Nationale Supérieure des Télécommunications, Paris, France (1999–2000). Between 2000 and 2005 he was a researcher at Technische Universitaet Berlin in the Telecommunication Networks Group. Since 2005 he has been full professor of computer science at the Technische Universität Ilmenau, leading the Telematics/Computer Networks research group. His research interests lie in the areas of network security, networking protocols, mobile communications and innovative communication services/architectures, and he regularly gives courses on network security, networking subjects and the basics of computer science (programming, algorithms etc.).

Michael Rossberg studied computer science at Technische Universitaet Ilmenau, Germany, from 2002 to 2007. Since 2007 he has been a researcher at the Telematics/Computer Networks research group. In 2011 he obtained his PhD in computer science with a thesis on peer-to-peer-based autoconfiguration of large-scale IPsec VPNs. His research interests lie in network security, resilience against denial-of-service attacks and performance evaluation/optimisation. Since December 2013 he has served as a lecturer in the Telematics and Computer Networks research group.

Preface to the second edition

Since the publication of the first edition of this book, 12 years ago, many developments have taken place in the field of network security. Indeed, the innovations are so numerous that we decided to develop this second edition of the book in a team, therefore Michael Rossberg and myself now jointly maintain the book.

The evolution of the topic required not only a rigorous revision of the existing chapters, but also the addition of new material in order to take new developments into account. For example, quite a number of new cryptographic algorithms are discussed in the new edition, including new attacks and security insights on former ones. Nevertheless, we decided to keep the discussion of some historic approaches, like DES and MD5, as they serve as a foundation of the newer developments and are well suited to explain important concepts. We extended the chapter on asymmetric cryptography with an introduction to cryptography based on elliptic curves, as this approach plays a more and more important practical role due to the improvements in calculating discrete logarithms. The chapter on mobile Internet communication and Mobile IP has been dropped from the second edition because Mobile IP has not been widely adopted in the open Internet, only in very controlled environments.

Furthermore, the book has been extended by the addition of a completely new part, which covers the protection of whole communications infrastructures against targeted attacks on integrity and availability. The chapter on Internet firewalls from the first edition has been integrated into this part of the book, for obvious reasons.

In its resulting structure this second edition serves well as a foundation for two or three consecutive college-level courses, but it is also possible to teach some aspects independently. For example, a three-step approach could cover IT security foundations (Part I) in a first course, their application to networks (Parts II and III) in a second course and the protection of communications infrastructures in a final third course, and it may be possible to attend the last course without the first and second ones. In this latter case, only some central ideas from the first part of the book need to be studied

first. A division into two lectures would cover essential parts of the first part of the book and discuss their application to networks. To cover all topics in the first three parts, one must plan for at least 4 hours of lectures per week. The protection of communications infrastructures would be the second independently held lecture in this case. We have had good experience with the two-step approach, which we have used for teaching at TU Ilmenau in recent years.

Please note that all chapters and sections in this book that are marked by an asterisk may safely be skipped during reading and teaching without impairing the understanding of subsequent material.

At this point we want to thank our students and the many other people who have helped us with their numerous questions and suggestions to present the teaching material in its current form. We would also like to thank two members of our research group who contributed slides to the lectures, which also served as a first foundation for the second edition of the book, Prof. Dr.-Ing. Thorsten Strufe and Dr.-Ing. Mathias Fischer. Prof. Dr. Martin Dietzfelbinger from the Complexity Theory and Efficient Algorithms research group provided us with valuable comments on our chapter on asymmetric cryptography, which we were largely able to integrate into this second edition. The responsibility for any errors that still might appear in the book despite all the help that was available, of course, lies with us. We will, therefore, continue to appreciate any comments or suggestions regarding the content of this book.

Ilmenau, July 2015
Guenter Schaefer and Michael Rossberg

Preface to the first edition

This book has evolved during my time as a technical assistant in the department of telecommunications networks at the Technical University of Berlin. It is based on my lecture Network Security that 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 Schmüger 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 staffs 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
Guenter Schaefer

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, the category of risks that evolve as a result of eavesdropping and the manipulation of data transmitted in communication networks and the vulnerability of the communication infrastructure itself. In particular, measures are discussed that can be taken to minimise them.

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 specific 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 most widely known one was probably the 'Caesar cipher', named after its creator Julius Caesar, in which each character of the alphabet

Security in Fixed and Wireless Networks, Second Edition.
Guenter Schaefer and Michael Rossberg.

Title of the German original: Netzsicherheit ISBN 978-3-86490-115-7

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*, that is, pure character replacement, and *transposition*, that is, changing the sequence 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 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 as well as 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 ciphering 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. Chapter 8 enlarges the topic in the context of scenarios with *group communication*. This deeper discussion may be skipped in an introductory course without impairing the understanding of further book chapters. Part 1 concludes with Chapter 9, 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 10, which examines general issues relating to the integration of security services in communication architectures. Chapter 11 discusses security protocols of the data link layer, Chapter 12 examines the security architecture for the Internet protocol *IPsec* and Chapter 13 closes Part 2 by describing security protocols for the transport layer.

Part 3 is devoted to wireless and mobile communication

Part 3 of the book presents the field of *secure wireless and mobile communication*. Chapter 14 differentiates the additional security aspects that arise in mobile communications 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 of the IEEE 802.11 standard for wireless local networks and includes an in-depth discussion of the weaknesses of former versions of the standard. Chapter 16 introduces the security functions for the current standards for mobile wide-area networks, that is, *GSM*, *UMTS* and *LTE*.

Part 4 deals with protection of communication infrastructures.

While Parts 1 to 3 of the book mainly concentrate on the security of communication processes between end systems, the fourth and last part of the book deals with *protection of large networks and the communication infrastructure*. Chapter 17 first describes the basic problem of protecting systems in open networks and provides a short overview of systematic threat analysis. It also discusses

the problem of protecting end systems as a requirement for secure network operation. Chapter 18 deals with *denial-of-service attacks*, which affect end systems as well as the communication infrastructure. Chapters 19 and 20 cover the security of fundamental communication infrastructure services: *routing* and *name resolution*. *Internet firewalls* as the main means for realising subnet-related access control are introduced in Chapter 21. Since attacks cannot always be prevented through the proactive security measures described in these chapters, it often makes sense to introduce additional control through *intrusion detection systems* and/or *intrusion prevention systems*. The principles of such systems and existing techniques are introduced in Chapter 22. Finally, Chapter 23 deals with difficulties in the management of large security infrastructures.

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 thus 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**.