

SECURITY

IN FIXED AND WIRELESS NETWORKS

an introduction to securing
data communications

Günter Schäfer

 **WILEY**

BIBLIOTHEQUE DU CERIST

IST 2956

Security in **Fixed** and **Wireless** **Networks**

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



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 accompanying website that contains support 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

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 Tunneling 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

17.4	Summary	351
17.5	Supplemental Reading	353
17.6	Questions	354
Bibliography		357
Abbreviations		373
Index		379