WILEY

TIMELY. PRACTICAL. RELIABLE.

Cryptography and Public Key Infrastructure on the Internet

Klaus Schmeh

IST 2836

Cryptography and Public Key Infrastructure on the Internet

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

Cryptography and Public Key Infrastructure on the Internet

Klaus Schmeh

Gesellschaft für IT-Sicherheit AG
Bochum, Germany

WILEY

BIBLIOTHEQUE DU CERIST

Copyright © 2001 by dpunkt.verlag GmbH, Heidelberg, Germany.
Title of the German original: *Kryptografie und Publik-Key-Infrastrukturen im Internet.* ISBN: 3 932588 90 8

English translation Copyright 2003 by John Wiley & Sons Ltd,

The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England. All rights reserved

National 01243 779777
International (+44) 1243 779777
e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on http://www.wileyeurope.com or http://www.wiley.com

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London W1T 4LP, UK, without the permission in writing of the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the publication. Requests to the Publisher should be addressed to the Permissions Department, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, or emailed to permreq@wiley.co.uk, or faxed to (+44) 1243 770571.

Neither the authors nor John Wiley & Sons, Ltd accept any responsibility or liability for loss or damage occasioned to any person or property through using the material, instructions, methods or ideas contained herein, or acting or refraining from acting as a result of such use. The authors and publisher expressly disclaim all implied warranties, including merchantability or fitness for any particular purpose. There will be no duty on the authors or publisher to correct any errors or defects in the software.

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Ltd is aware of a claim, the product names appear in capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

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

1775

Library of Congress Cataloging-in-Publication Data

(to follow)

British Library Cataloguing in Publication Data

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

ISBN 0 470 84745 X
Translated and typeset by Cybertechnics Ltd, Sheffield
Printed and bound in Great Britain by Biddles Ltd., Guildford and Kings Lynn
This book is printed on acid-free paper responsibly manufactured from sustainable forestry
for which at least two trees are planted for each one used for paper production.

Contents

Foreword by Carl Ellison xi

PART 1 WHY CRYPTOGRAPHY ON THE INTERNET? 1

1 Introduction 3
- 1.1 If the Internet were a car ... 3
- 1.2 Security on the Internet 4
- 1.3 The second edition 6
- 1.4 Why yet another cryptography book? 6
- 1.5 My regrets, my requests and my thanks 8

2 What is cryptography and why is it so important? 9
- 2.1 The name of the game 9
- 2.2 Why is cryptography so important? 13
- 2.3 Uses of cryptography 15
- 2.4 And who the devil is Alice? 16
- 2.5 Summary 17

3 How is it possible to eavesdrop on the Internet? 19
- 3.1 The structure of the Internet 20
- 3.2 How is it possible to eavesdrop on the Internet? 24
- 3.3 Some practical examples 36
- 3.4 Summary 38

PART 2 THE PRINCIPLES OF CRYPTOGRAPHY 39

4 Symmetric encryption 41
- 4.1 What is symmetric encryption? 42
- 4.2 Elementary encryption methods 46
- 4.3 Polyalphabetic ciphers 49
- 4.4 The Enigma and other rotor cipher machines 52

5 Modern symmetric encryption algorithms 59
- 5.1 The Data Encryption Standard (DES) 59
- 5.2 Other symmetrical ciphers 67
- 5.3 AES 75

BIBLIOTHEQUE DU CERIST

6 Asymmetrical encryption 83
- 6.1 The key exchange problem 83
- 6.2 A little maths 86
- 6.3 One-way functions and trapdoor functions 92
- 6.4 The Diffie–Hellman key exchange 93
- 6.5 RSA 95
- 6.6 Other asymmetrical algorithms 100
- 6.7 Hybrid algorithms 101
- 6.8 Differences between public and secret key 102

7 Digital signatures 105
- 7.1 What is a digital signature? 105
- 7.2 RSA as a signature algorithm 106
- 7.3 Signatures based on the discrete logarithm 107
- 7.4 Security of signature algorithms 111
- 7.5 Differences between DLSSs and RSA 112
- 7.6 Other signature algorithms 113

8 Cryptographic hash functions 115
- 8.1 What is a cryptographic hash function? 116
- 8.2 The most important cryptographic hash functions 123
- 8.3 Key-dependent hash functions 128
- 8.4 Further applications 129

9 Cryptographic random generators 131
- 9.1 Random numbers in general 132
- 9.2 Random numbers in cryptography 132
- 9.3 The most important pseudo-random generators 136
- 9.4 Stream ciphers 139
- 9.5 Prime number generators 143

PART 3 ADVANCED CRYPTOGRAPHY 145

10 Standardisation in cryptography 147
- 10.1 Standards 147
- 10.2 Standards in the real world 149
- 10.3 What you ought to know about standards 150
- 10.4 PKCS standards 150
- 10.5 IEEE P1363 153

11 Block cipher modes of operation and data transformation for asymmetrical algorithms 155
- 11.1 Block cipher modes of operation 155
- 11.2 Data transformation for the RSA algorithm 160

12 Cryptographic protocols 165
- 12.1 Protocols 165
- 12.2 Protocol properties 168
- 12.3 Protocols in cryptography 170
- 12.4 Attributes of cryptographic protocols 170

12.5 Attacks on cryptographic protocols 173
12.6 An example of a protocol: blind signatures 177
12.7 Other protocols 178

13 Authentication 179
13.1 Authentication and identification 179
13.2 Authentication procedures 180
13.3 Biometric authentication 183
13.4 Authentication on the Internet 191
13.5 Kerberos 197
13.6 RADIUS and TACACS 199
13.7 Packaging of authentication mechanisms 202

14 Cryptosystems based on elliptic curves 205
14.1 Mathematical principles 205
14.2 Cryptosystems based on elliptic curves 208
14.3 Examples and standards for ECCs 209

15 Implementing cryptography 213
15.1 Crypto hardware and software 213
15.2 Smart cards 215
15.3 Other crypto hardware 220
15.4 Crypto software 223
15.5 Universal crypto interfaces 226
15.6 Real-world attacks 229
15.7 Evaluation and certification 233

PART 4 PUBLIC KEY INFRASTRUCTURES 237

16 Public key infrastructures 239
16.1 Trust models in public key cryptography 239
16.2 Variants of hierarchical PKIs 247
16.3 PKI standards 249

17 How a PKI works 255
17.1 Components of a PKI 255
17.2 Certificate management 260
17.3 Enrolment 263
17.4 Certificate policy and CPS 265

18 Digital certificates 269
18.1 X.509v1 certificates 270
18.2 X.509v2 certificates 270
18.3 PKCS#6 certificates 271
18.4 X.509v3 certificates 272
18.5 The PKIX and ISIS X.509v3 extensions 275
18.6 Attribute certificates 276
18.7 X.509 summary 278
18.8 PGP certificates 278

BIBLIOTHEQUE DU CERIST

19 Certificate servers 281
19.1 Directory service 281
19.2 Certificate servers and directory services 285
19.3 Requesting certificate revocation information 286

20 Practical aspects of PKI construction 295
20.1 The course of the construction of a PKI 295
20.2 Basic questions about PKI construction 296
20.3 The most important PKI suppliers 300

PART 5 CRYPTO PROTOCOLS FOR THE INTERNET 309

21 The Internet and the OSI model 311
21.1 The OSI model 311
21.2 In which layer can encryption be undertaken? 315

22 Crypto standards for OSI Layers 1 and 2 321
22.1 Crypto extensions for ISDN (Layer 1) 321
22.2 Cryptography in the GSM standard (Layer 1) 323
22.3 Crypto extensions for PPP (Layer 2) 325
22.4 Virtual private networks 327

23 IPSec (Layer 3) 333
23.1 IPSec and IKE 333
23.2 IPSec 334
23.3 IKE 336
23.4 SKIP 339
23.5 Critical assessment of IPSec 340
23.6 Virtual private networks with IPSec 341

24 SSL, TLS and WTLS (Layer 4) 343
24.1 SSL working method 344
24.2 SSL protocol operation 345
24.3 Successful SSL 347
24.4 Technical comparison between IPSec and SSL 347
24.5 WTLS 348

25 Cryptographic standards for the World Wide Web (Layer 7) 351
25.1 Basic Authentication 352
25.2 Digest Access Authentication 352
25.3 HTTP on top of SSL (HTTPS) 353
25.4 Digital signatures on the World Wide Web 354
25.5 Sundries 357

26 E-mail encryption standards (Layer 7) 359
26.1 E-mails on the Internet 359
26.2 PEM 361
26.3 OpenPGP 363
26.4 S/MIME 365
26.5 Mailtrust 367

BIBLIOTHEQUE DU CERIST

26.6 Which standard is standard? 369
26.7 Retrieving e-mails: POP and IMAP 370

27 Internet payment systems (Layer 7) 373
27.1 Internet payment systems in general 373
27.2 Credit card systems 374
27.3 Account systems 378
27.4 Cash systems 380
27.5 The payment system crisis 384

28 Further Application Layer protocols 385
28.1 Secure Shell (SecSH) 385
28.2 SASL 387
28.3 Crypto extensions for SNMP 388
28.4 Online banking with HBCI 389
28.5 Crypto extensions for SAP R/3 391

PART 6 MORE ABOUT CRYPTOGRAPHY 393

29 Political aspects of cryptography 395
29.1 How governments control encryption 396
29.2 The German signature law 400
29.3 Cryptography and policy in the USA 404

30 People who play a role in cryptography 407
30.1 The ten most important people 407
30.2 The ten most important companies 413
30.3 The ten most important non-profit organisations 417

31 Where to find out more about cryptography 423
31.1 The ten most important sources of information 423
31.2 The ten most important cryptography books 426
31.3 The ten most important Web sites 430

32 The last chapter 433
32.1 The ten greatest crypto flops 433
32.2 Ten indications of snake oil 437
32.3 Ten examples of snake oil 439
32.4 Ten popular crypto misapprehensions 443
32.5 Murphy's ten laws of cryptography 445

Appendix A: List of abbreviations 447
Appendix B: Bibliography 453
Index 463

BIBLIOTHEQUE DU CERIST