

Handbook of Communications Security

About the Author



Fabio Garzia is Professor of various subjects regarding security in the Safety & Security and Civil Protection Masters Program at the University of Rome "La Sapienza" and in other Masters programs at the same university and at other universities in Italy. He is also an Adjunct Professor at Wessex Institute of Technology (UK), and a member of the European Academy of Science and Arts (Salzburg, Austria).

He is the author of more than 100 scientific papers published in various international journals and conference proceedings and author or editor of several books regarding security, both in Italian and

English. He is co-editor of the International Journal of Safety & Security Engineering (WIT Press). He serves as a reviewer for various international scientific journals, as a member of various committees and working groups regarding security and ICT, a member of the Scientific Committees of various international conferences, a member of the Executive Committee of IEEE International Carnahan Conference on Security Technology, and as co-Chairman of the Safety & Security Engineering conference series.

A consultant, designer, construction manager and tester of security and ICT systems, he has worked or is still working for: Vatican City State, Senate of Italian Republic, Gran Sasso mountain INFN underground laboratories, Italian Space Agency, high velocity railway, high security sites, airports, ports, rail stations, museum, basilicas, different public and private subjects, etc. He is an Expert Member of the Board of Public Works of Italy.

Handbook of Communications Security

F. Garzia

University of Rome "La Sapienza" Italy

WITPRESS Southampton, Boston



F. Garzia

University of Rome "La Sapienza" Italy

Published by

WIT Press

Ashurst Lodge, Ashurst, Southampton, SO40 7AA, UK

Tel: 44 (0) 238 029 3223; Fax: 44 (0) 238 029 2853

E-Mail: witpress@witpress.com

<http://www.witpress.com>

For USA, Canada and Mexico

WIT Press

25 Bridge Street, Billerica, MA 01821, USA

Tel: 978 667 5841; Fax: 978 667 7582

E-Mail: infousa@witpress.com

<http://www.witpress.com>

British Library Cataloguing-in-Publication Data

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

ISBN: 978-1-84564-768-1

eISBN: 978-1-84564-769-8

Library of Congress Catalog Card Number: 2012954752

No responsibility is assumed by the Publisher, the Editors and Authors for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. The Publisher does not necessarily endorse the ideas held, or views expressed by the Editors or Authors of the material contained in its publications.

©WIT Press 2013. All rights reserved.

Printed by Lightning Source, UK.

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, or otherwise, without the prior written permission of the Publisher.

CONTENTS

Preface	xix
Introduction.....	1
Chapter 1 Fundamentals of Telecommunications.....	3
1.1 Introduction	3
1.1.1 Mode of network operation.....	3
1.1.2 Network hardware	3
1.1.3 Network software	8
1.1.4 Reference models.....	11
1.1.5 Examples of network.....	15
1.1.6 International entities of the telecommunications world.....	22
1.2 The physical layer	24
1.2.1 Signals theory.....	24
1.2.2 Transmission over guided media	46
1.2.3 Wireless transmission	48
1.2.4 Satellite transmission	50
1.2.5 Fixed telephone network	51
1.2.6 The cellular telephone network	52
1.3 Data link physical layer	55
1.4 Medium Access Control sub-layer.....	57
1.4.1 Wireless networks	62
1.4.2 Switching in the data link layer.....	74
1.5 The network layer.....	79
1.5.1 Routing algorithms	81
1.5.2 Congestion control algorithms	84
1.5.3 Quality of service	86
1.5.4 Connection between networks.....	87
1.5.5 The layer network on the Internet	88
1.6 The transport layer.....	96

1.6.1 The UDP transport protocol on the Internet	99
1.6.2 The TCP transport protocol on the Internet	99
1.6.3 Performance on networks	104
1.7 The session layer	108
1.8 The presentation layer	109
1.9 The application layer.....	109
1.9.1 The domain name system.....	110
1.9.2 Email.....	111
1.9.3 The World Wide Web.....	113
1.9.4 Multimedia	124
Chapter 2 Cryptography	137
2.1 Introduction	137
2.2 General elements of cryptography.....	141
2.2.1 Replacement ciphers and transposition ciphers	141
2.2.2 XOR operation.....	142
2.2.3 One-time pad.....	143
2.2.4 Computer algorithms	144
2.2.5 Introduction to protocols.....	144
2.2.6 Communication by symmetric cryptography.....	147
2.2.7 One-way functions.....	147
2.2.8 One-way hash functions	148
2.2.9 Communication by public-key cryptography.....	148
2.2.10 Hybrid cryptosystems	149
2.2.11 Digital signature	149
2.2.12 Digital signatures with encryption.....	153
2.2.13 Generation of random or pseudo-random sequences.....	153
2.2.14 Exchange of keys.....	154
2.2.15 Authentication.....	157
2.2.16 Authentication and key exchange.....	158
2.2.17 Multiple public-key cryptography.....	158
2.2.18 Division of a secret	159
2.2.19 Secret sharing	159
2.2.20 Cryptographic protection of archives	160
2.2.21 Stamping services	160
2.2.22 Delegated signature	161
2.2.23 Group signature	161
2.2.24 Key escrow.....	162
2.2.25 Digitally certified email	162
2.2.26 Length of the symmetric key.....	162
2.2.27 Public-key length.....	164
2.2.28 Comparison between the length of the symmetric key and the length of the public key... 165	
2.2.29 Birthday attacks in relation to one-way functions.....	165
2.2.30 Optimal key length	165

2.2.31 Key management	166
2.2.32 Key generation	166
2.2.33 Key transfer	168
2.2.34 Key verification	168
2.2.35 Using keys	168
2.2.36 Key update	169
2.2.37 Key storage	169
2.2.38 Compromising of keys	169
2.2.39 Lifespan of keys	170
2.2.40 Destruction of keys	170
2.2.41 Key management in public-key systems	171
2.2.42 Algorithm types and modes	171
2.2.43 Use of algorithms	175
2.3 Elements of basic maths for cryptography	178
2.3.1 Information theory	178
2.3.2 Complexity theory	180
2.3.3 Numbers theory	181
2.3.4 Factorisation	185
2.3.5 The generation of prime numbers	186
2.3.6 Discrete logarithms in finite fields	186
2.4 Data Encryption Standard	187
2.4.1 The DES algorithm	187
2.4.2 Security of DES	191
2.4.3 Differential and linear analysis	193
2.4.4 DES variants	195
2.5 Other block ciphers	196
2.6 Cipher combination	196
2.6.1 Double encryption	197
2.6.2 Triple encryption	197
2.6.3 Whitening	197
2.6.4 Cascading	197
2.7 Pseudo-random sequence generators and flow ciphers	197
2.7.1 Congruent linear generators	197
2.7.2 Linear shift records with feedback	198
2.7.3 Design and analysis of stream ciphers	199
2.7.4 Stream ciphers based on LFSR	199
2.7.5 A5 stream cipher	199
2.7.6 Additive generators	200
2.7.7 PKZIP	200
2.7.8 Design of stream ciphers	200
2.7.9 Generation of multiple streams from a single pseudo-random generator	200
2.8 Real random sequence generators	201
2.8.1 Random noise	201

2.8.2 Computer clock.....	202
2.8.3 Keyboard latency typing	202
2.8.4 Polarisation and correlation.....	202
2.8.5 Distillation of randomness.....	203
2.9 One-way hash functions.....	203
2.9.1 Use of the symmetric block algorithms for generation of one-way hash functions.....	204
2.9.2 Use of public-key algorithms for the generation of one-way hash functions.....	204
2.9.3 Message authentication code.....	205
2.10 Advanced Encryption Standard.....	205
2.10.1 Introduction to AES	205
2.10.2 Preliminary concepts.....	206
2.10.3 Description of the algorithm.....	210
2.10.4 Rational schema	211
2.10.5 Encryption	212
2.10.6 Key expansion function.....	212
2.10.7 Decryption.....	213
2.10.8 Security	213
2.11 Public-key algorithms	214
2.11.1 The RSA algorithm.....	215
2.11.2 Elliptic curve cryptosystems	217
2.11.3 Other public-key cryptosystems	217
2.12 Public-key algorithms for digital signature.....	217
2.12.1 Digital signature algorithm.....	217
2.12.2 Digital signature via discrete logarithms.....	219
2.12.3 Other algorithms for digital signature	219
2.13 Algorithms for the exchange of keys.....	220
2.13.1 Diffie–Hellman	220
2.13.2 Station–station protocol	221
2.13.3 Exchange of encrypted keys.....	221
2.14 Quantum cryptography.....	222
2.15 Practical applications	223
2.15.1 Management protocol of secret IBM keys	223
2.15.2 STU-III.....	224
2.15.3 Kerberos.....	224
2.15.4 Kryptonight.....	225
2.15.5 SESAME.....	225
2.15.6 IBM common cryptographic architecture	225
2.15.7 ISO Authentication	226
2.15.8 Privacy Enhanced Mail	228
2.15.9 TIS/PEM.....	228
2.15.10 Message Security Protocol.....	228
2.15.11 Pretty Good Privacy.....	229
2.15.12 Smart card.....	229

2.15.13 Public-key cryptographic standards	230
2.15.14 CLIPPER.....	230
2.15.15 CAPSTONE	230
2.15.16 Other systems.....	231
Chapter 3 Steganography	233
3.1 Introduction.....	233
3.2 History of steganography.....	233
3.2.1 The Egyptians	233
3.2.2 The Greeks	233
3.2.3 The Chinese.....	234
3.2.4 Gaspar Schott	234
3.2.5 Johannes Trithemius.....	234
3.2.6 Giovanni Porta	234
3.2.7 GirolamoCardano	234
3.2.8 Blaise de Vigenere.....	235
3.2.9 Auguste Kerckhoffs.....	235
3.2.10 Bishop John Wilkins.....	235
3.2.11 Mary Queen of Scots.....	235
3.2.12 George Washington.....	235
3.2.13 Air mail by pigeons in Paris in 1870.....	236
3.2.14 The First World War.....	236
3.2.15 The Second World War.....	236
3.2.16 The Vietnam War.....	237
3.2.17 Margaret Thatcher	237
3.3 Principles of steganography.....	237
3.3.1 The background to secret communication	237
3.3.2 Steganographic security systems.....	241
3.3.3 The concealment of information in data noise.....	242
3.3.4 Adaptive and non-adaptive algorithms.....	243
3.3.5 Active and malicious hackers	243
3.3.6 Concealment of information within written text.....	245
3.3.7 Examples of invisible communication	246
3.4 The principal steganographic techniques	246
3.4.1 Preliminary definitions	247
3.4.2 Substitution methods	247
3.4.3 Methods for domain transformation	251
3.4.4 Spread spectrum methods	254
3.4.5 Statistical methods	256
3.4.6 Distortion methods	256
3.5 Steganalysis.....	257
3.6 Practical examples	259
3.6.1 Cryptapix.....	260
3.6.2 Data stash.....	261

3.6.3 Hermeticstego	262
3.6.4 Hide in picture – Blowfish.....	263
3.6.5 Hide in picture – Rijndael.....	264
3.6.6 OpenPuff	265
3.6.7 S tools – Data Encryption Standard (DES).....	266
3.6.8 S tools – International Data Encryption Algorithm (IDEA).....	267
3.6.9 S tools – MDC	268
3.6.10 S tools – Triple DES	269
3.6.11 SilentEye	270
Chapter 4 Digital Watermarking	271
4.1 Introduction	271
4.2 History and terminology	271
4.3 Basic principles	272
4.4 Applications	273
4.5 Algorithm requirements	274
4.6 Evaluation of systems	275
4.7 Watermark removal algorithms	278
4.8 Future evolution and standardization	278
4.9 Watermarking technologies.....	279
4.9.1 Selection of pixels or blocks	279
4.9.2 Work selection space	280
4.9.3 Formatting of the watermarking signal.....	283
4.9.4 Fusion of the message in the document to be watermarked	284
4.9.5 Optimisation of the watermark detector	284
4.9.6 Watermarking of video images.....	285
4.10 Strength requirements	285
4.10.1 Signal decrease.....	286
4.10.2 Malfunction of the watermarking detector	287
4.10.3 Watermark counterfeiting.....	288
4.10.4 Watermark detection	290
4.10.5 System architectures	290
4.11 Digital fingerprint	291
Chapter 5 Security in Wired Networks.....	293
5.1 Introduction	293
5.2 Introduction to security policies and risk analysis.....	294
5.3 Firewall.....	297
5.3.1 Design of a firewall	299
5.3.2 Limits of firewalls.....	300
5.3.3 Risk regions.....	300
5.3.4 Introduction to firewalls	301
5.3.5 Types of firewalls.....	302
5.3.6 Firewall architectures.....	306

5.3.7 Further types of firewalls	307
5.3.8 Firewall selection.....	317
5.3.9 Further firewall considerations	320
5.3.10 Location of firewalls	323
5.3.11 Network security assessments.....	324
5.4 The S-HTTP protocol.....	327
5.4.1 Introduction to S-HTTP.....	328
5.4.2 Digital signatures in S-HTTP	331
5.5 Secure Socket Layer	333
5.5.1 Features of browsers and SSL servers.....	336
5.5.2 Tunnels in firewalls and SSL	337
5.5.3 S/MIME: secure extensions.....	338
5.6 Intrusion detection.....	339
5.6.1 Installation of an IDS on a host.....	342
5.6.2 IDS fusion.....	343
5.6.3 Configuration of an IDS	344
5.7 Network attacks.....	346
5.7.1 Denial-of-service attack	346
5.7.2 Number sequence anticipation attack.....	346
5.7.3 TCP protocol hijack	348
5.7.4 Sniffer attack.....	348
5.7.5 Active desynchronisation attack	349
5.7.6 Spoofing attack.....	353
5.7.7 Hyperlink spoofing.....	355
5.7.8 Web spoofing.....	355
5.8 Authentication	358
5.9 Virtual Private Networks.....	360
5.9.1 The choice of a VPN.....	363
5.9.2 Various VPN solutions	364
5.9.3 Setting up a VPN	365
5.10 The exchange of Kerberos keys on distributed systems.....	365
5.10.1 Ticket flags.....	372
5.10.2 Kerberos archive	374
5.10.3 Vulnerability of Kerberos.....	375
5.11 Security of commercial transactions on the Internet	376
5.11.1 Use of credit cards on the Internet.....	380
5.11.2 The Secure Electronic Transmission protocol.....	381
5.12 Audit trails.....	382
5.13 Java language and related security aspects	384
5.14 Web browser security.....	387
5.14.1 Simple attacks on Web browsers	389
5.14.2 ActiveX components and associated security issues	389
5.14.3 Web cookies.....	391

5.15 Scripts and security issues	392
5.15.1 CGI scripts	392
5.15.2 The languages used for creating scripts.....	395
5.15.3 Perl language.....	396
5.15.4 CGI scripts and security issues	397
5.16 Computer viruses and security policies	399
5.16.1 Replication	400
5.16.2 Concealment.....	402
5.16.3 Bomb	404
5.16.4 Worm virus	405
5.16.5 Trojan horses	406
5.16.6 Virus prevention	406
5.16.7 Virus protection.....	409
5.17 Analysis of attacks	411
5.17.1 Execution of the attack	416
5.18 Prevention of attacks.....	420
5.19 Disaster prevention and recovery	421
5.19.1 Division of disasters.....	421
5.19.2 Network disasters	421
5.19.3 Server disasters.....	427
5.19.4 Disaster simulation	432
5.20 Network security policy.....	432
Chapter 6 Security of Wireless Networks	445
6.1 Introduction	445
6.2 Introduction to wireless networks	445
6.2.1 The propagation of electromagnetic waves	446
6.2.2 The signal-to-noise ratio	448
6.2.3 The main players that operate on wireless	449
6.3 Risks and threats in the wireless industry	449
6.3.1 Objectives of the information theory.....	449
6.3.2 Analysis.....	450
6.3.3 Spoofing	450
6.3.4 Denial-of-service.....	451
6.3.5 Malicious codes	451
6.3.6 Social engineering	451
6.3.7 Rogue access points.....	452
6.3.8 Security of cellular telephony.....	452
6.3.9 Hacking and hackers in the wireless industry	453
6.3.10 Radio frequency identification.....	456
6.4 Wireless technologies in the physical layer	456
6.4.1 The industrial, scientific and medical band	457
6.4.2 Modulation techniques used.....	457
6.5 Frame management in the wireless industry	458

6.5.1 Beacon	459
6.5.2 Probe request.....	459
6.5.3 Probe response.....	459
6.5.4 Authentication	459
6.5.5 Association request.....	460
6.5.6 Association response	460
6.5.7 Disassociation and de-authentication	460
6.5.8 Carrier sense multiple access/collision avoidance	460
6.5.9 Fragmentation	462
6.5.10 Distributed coordination function	462
6.5.11 Point coordination function.....	463
6.5.12 Interframe spacing.....	463
6.5.13 Service set identifier	463
6.6 Local wireless networks and personal wireless networks.....	464
6.6.1 Ad hoc mode.....	464
6.6.2 Infrastructure mode.....	464
6.6.3 Bridging.....	465
6.6.4 Repeater.....	465
6.6.5 Mesh networks	466
6.6.6 Wireless LAN standards	466
6.6.7 Personal area networks.....	467
6.7 Wireless WAN technology.....	475
6.7.1 Cellular phone technology.....	475
6.7.2 GPS technology	491
6.7.3 TETRA technology	492
6.7.4 Wireless Application Protocol	495
6.8 Wireless antennae.....	500
6.8.1 Introduction to antennae for wireless devices.....	500
6.8.2 Fresnel zone.....	502
6.8.3 Types of antennae.....	503
6.9 The implementation of wireless networks.....	504
6.9.1 Requirement acquisition.....	504
6.9.2 Cost estimate	505
6.9.3 Evaluation of investment	505
6.9.4 Site analysis	506
6.9.5 Network design	509
6.9.6 Device verification.....	509
6.9.7 Development and installation	509
6.9.8 Certification	510
6.9.9 Audit	510
6.10 Wireless devices.....	510
6.10.1 Access points.....	510
6.10.2 Mobile user devices	511

6.11 The security of wireless LANS.....	513
6.11.1 History of wireless security.....	514
6.11.2 Authentication.....	514
6.11.3 SSID.....	516
6.11.4 Foundations of wireless security.....	516
6.11.5 WEP.....	516
6.11.6 802.1x.....	518
6.11.7 RADIUS.....	520
6.11.8 EAP.....	521
6.11.9 WPA.....	528
6.11.10 802.11i.....	529
6.11.11 WPA2.....	534
6.11.12 WAPI.....	534
6.11.13 Detection of false access points.....	535
6.12 Violation of wireless security.....	535
6.12.1 The process of attack.....	536
6.12.2 Breach technologies.....	538
6.12.3 Access point breach techniques.....	543
6.13 Wireless security policies.....	545
6.13.1 Introduction to security policies.....	545
6.13.2 Drafting of security policies.....	546
6.13.3 Risk assessment.....	547
6.13.4 Impact analysis.....	548
6.13.5 The areas of wireless security policies.....	548
6.14 Wireless security architectures.....	551
6.14.1 Static WEP.....	551
6.14.2 VPN.....	553
6.14.3 Wireless gateway.....	556
6.14.4 802.1x.....	558
6.14.5 Comparison between the different wireless architectures.....	559
6.15 Wireless tools.....	561
6.15.1 Scanning tools.....	562
6.15.2 Sniffing tools.....	562
6.15.3 Hybrid tools.....	562
6.15.4 DoS tools.....	563
6.15.5 Cracking tools.....	563
6.15.6 Access points attack tools.....	563
6.15.7 Security tools.....	563
Chapter 7 Voice Security	565
7.1 Introduction.....	565
7.2 Characteristics of the spoken language.....	565
7.2.1 The structure of language.....	567
7.2.2 Phonemes and phones.....	567

7.3 Voice configuration.....	567
7.3.1 The classic source–filter model.....	567
7.3.2 The general source–filter model.....	568
7.3.3 Linear prediction modeling.....	569
7.4 The transmission of voice signals	570
7.5 Voice signal encryption	572
7.5.1 Voice signal analogue encryption	573
7.5.2 Digital encryption of voice signals.....	580
7.6 Voice source encoding.....	581
7.6.1 The formant vocoder	581
7.6.2 The channel vocoder	581
7.6.3 The vocoder based on linear prediction.....	582
7.6.4 The sinusoidal model	585
7.6.5 Standards	585
7.7 Voice cryptanalysis.....	585
7.7.1 Tools and parameters for voice cryptanalysis	586
7.7.2 Using the spectrograph for cryptanalysis	586
7.7.3 Analogue methods.....	587
7.7.4 Cryptanalysis of digital ciphers.....	588
7.7.5 Linear prediction vocoder cryptanalysis.....	588
7.8 VoIP systems security.....	588

Chapter 8 Protection from Bugging.....593

8.1 Introduction.....	593
8.2 Devices for environmental bugging	594
8.2.1 Bugging devices and miniature cameras.....	594
8.2.2 Directional microphones	599
8.2.3 Environmental bugging using laser devices	600
8.2.4 Trackers using GPS technology.....	600
8.2.5 Mobile phone bugging devices	601
8.2.6 Other devices.....	602
8.2.7 Stethoscopic microphones	602
8.2.8 Miniature audio and video recorders	602
8.2.9 Keystroke recorders on a computer keyboard (key catcher)	602
8.2.10 Bugging software for computers	603
8.2.11 Portable document scanners	603
8.3 Devices and techniques for protection against environmental bugging.....	604
8.3.1 Scanners.....	604
8.3.2 Broadband bugging device detectors.....	605
8.3.3 Bugging device detectors based on cellular technology.....	606
8.3.4 Spectrum analysers	607
8.3.5 Multifunction spectrum analysers	609
8.3.6 Multifunction devices.....	609
8.3.7 Non-linear junction detectors	610

8.3.8 Hidden miniature camera detectors	614
8.3.9 Wireless remote camera detectors	614
8.3.10 Electromagnetic jammers	615
8.3.11 Jammers for audio devices.....	615
8.3.12 Jammers for laser beam bugging devices	616
8.3.13 Encrypted phones.....	616
8.3.14 Software utilities	617
8.3.15 TEMPEST	617
8.4 Procedures and guidelines for suspected environmental bugging.....	619
Bibliography	623
Index.....	635