

Handbook of Information and Communication Security

Bearbeitet von
Peter Stavroulakis, Mark Stamp

1st Edition. 2010. Buch. xvi, 867 S. Hardcover
ISBN 978 3 642 04116 7
Format (B x L): 15,5 x 23,5 cm

[Weitere Fachgebiete > Technik > Technische Instrumentierung > Technische Zuverlässigkeit, Sicherheitstechnik](#)

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, red, sans-serif font. Above the 'i' in 'shop' are three red dots of varying sizes, arranged in a slight arc. Below the main text, the words 'DIE FACHBUCHHANDLUNG' are written in a smaller, red, all-caps, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Contents

Part A Fundamentals and Cryptography

1	A Framework for System Security	3
	<i>Clark Thomborson</i>	
1.1	Introduction	3
1.2	Applications	13
1.3	Dynamic, Collaborative, and Future Secure Systems	18
	References	19
	The Author	20
2	Public-Key Cryptography	21
	<i>Jonathan Katz</i>	
2.1	Overview	21
2.2	Public-Key Encryption: Definitions	23
2.3	Hybrid Encryption	26
2.4	Examples of Public-Key Encryption Schemes	27
2.5	Digital Signature Schemes: Definitions	30
2.6	The Hash-and-Sign Paradigm	31
2.7	RSA-Based Signature Schemes	32
2.8	References and Further Reading	33
	References	33
	The Author	34
3	Elliptic Curve Cryptography	35
	<i>David Jao</i>	
3.1	Motivation	35
3.2	Definitions	36
3.3	Implementation Issues	39
3.4	ECC Protocols	41
3.5	Pairing-Based Cryptography	44
3.6	Properties of Pairings	46
3.7	Implementations of Pairings	48
3.8	Pairing-Friendly Curves	54
3.9	Further Reading	55
	References	55
	The Author	57

4	Cryptographic Hash Functions	59
	<i>Praveen Gauravaram and Lars R. Knudsen</i>	
4.1	Notation and Definitions	60
4.2	Iterated Hash Functions	61
4.3	Compression Functions of Hash Functions	62
4.4	Attacks on Hash Functions	64
4.5	Other Hash Function Modes	66
4.6	Indifferentiability Analysis of Hash Functions	68
4.7	Applications	69
4.8	Message Authentication Codes	70
4.9	SHA-3 Hash Function Competition	73
	References	73
	The Authors	79
5	Block Cipher Cryptanalysis	81
	<i>Christopher Swenson</i>	
5.1	Breaking Ciphers	81
5.2	Differential Cryptanalysis	85
5.3	Conclusions and Further Reading	88
	References	89
	The Author	89
6	Chaos-Based Information Security	91
	<i>Jerzy Pejaś and Adrian Skrobek</i>	
6.1	Chaos Versus Cryptography	92
6.2	Paradigms to Design Chaos-Based Cryptosystems	93
6.3	Analog Chaos-Based Cryptosystems	94
6.4	Digital Chaos-Based Cryptosystems	97
6.5	Introduction to Chaos Theory	100
6.6	Chaos-Based Stream Ciphers	103
6.7	Chaos-Based Block Ciphers	113
6.8	Conclusions and Further Reading	123
	References	124
	The Authors	128
7	Bio-Cryptography	129
	<i>Kai Xi and Jiankun Hu</i>	
7.1	Cryptography	129
7.2	Overview of Biometrics	138
7.3	Bio-Cryptography	145
7.4	Conclusions	154
	References	155
	The Authors	157
8	Quantum Cryptography	159
	<i>Christian Monyk</i>	
8.1	Introduction	159
8.2	Development of QKD	160
8.3	Limitations for QKD	164
8.4	QKD-Network Concepts	165
8.5	Application of QKD	168

8.6	Towards ‘Quantum-Standards’	170
8.7	Aspects for Commercial Application	171
8.8	Next Steps for Practical Application	173
	References	174
	The Author	174
 Part B Intrusion Detection and Access Control		
9	Intrusion Detection and Prevention Systems	177
	<i>Karen Scarfone and Peter Mell</i>	
9.1	Fundamental Concepts	177
9.2	Types of IDPS Technologies	182
9.3	Using and Integrating Multiple IDPS Technologies	190
	References	191
	The Authors	192
10	Intrusion Detection Systems	193
	<i>Bazara I. A. Barry and H. Anthony Chan</i>	
10.1	Intrusion Detection Implementation Approaches	193
10.2	Intrusion Detection System Testing	196
10.3	Intrusion Detection System Evaluation	201
10.4	Summary	203
	References	204
	The Authors	205
11	Intranet Security via Firewalls	207
	<i>Inderjeet Pabla, Ibrahim Khalil, and Jiankun Hu</i>	
11.1	Policy Conflicts	207
11.2	Challenges of Firewall Provisioning	209
11.3	Background: Policy Conflict Detection	210
11.4	Firewall Levels	213
11.5	Firewall Dependence	213
11.6	A New Architecture for Conflict-Free Provisioning	213
11.7	Message Flow of the System	216
11.8	Conclusion	217
	References	218
	The Authors	218
12	Distributed Port Scan Detection	221
	<i>Himanshu Singh and Robert Chun</i>	
12.1	Overview	221
12.2	Background	222
12.3	Motivation	223
12.4	Approach	225
12.5	Results	230
12.6	Conclusion	231
	References	233
	The Authors	234
13	Host-Based Anomaly Intrusion Detection	235
	<i>Jiankun Hu</i>	
13.1	Background Material	236

13.2	Intrusion Detection System	239
13.3	Related Work on HMM-Based Anomaly Intrusion Detection	245
13.4	Emerging HIDS Architectures	250
13.5	Conclusions	254
	References	254
	The Author	255
14	Security in Relational Databases	257
	<i>Neerja Bhatnagar</i>	
14.1	Relational Database Basics	258
14.2	Classical Database Security	260
14.3	Modern Database Security	263
14.4	Database Auditing Practices	269
14.5	Future Directions in Database Security	270
14.6	Conclusion	270
	References	271
	The Author	272
15	Anti-bot Strategies Based on Human Interactive Proofs	273
	<i>Alessandro Basso and Francesco Bergadano</i>	
15.1	Automated Tools	273
15.2	Human Interactive Proof	275
15.3	Text-Based HIPs	276
15.4	Audio-Based HIPs	278
15.5	Image-Based HIPs	279
15.6	Usability and Accessibility	288
15.7	Conclusion	289
	References	289
	The Authors	291
16	Access and Usage Control in Grid Systems	293
	<i>Maurizio Colombo, Aliaksandr Lazouski, Fabio Martinelli, and Paolo Mori</i>	
16.1	Background to the Grid	293
16.2	Standard Globus Security Support	294
16.3	Access Control for the Grid	295
16.4	Usage Control Model	300
16.5	Sandhu's Approach for Collaborative Computing Systems	302
16.6	GridTrust Approach for Computational Services	303
16.7	Conclusion	305
	References	306
	The Authors	307
17	ECG-Based Authentication	309
	<i>Fahim Sufi, Ibrahim Khalil, and Jiankun Hu</i>	
17.1	Background of ECG	310
17.2	What Can ECG Based Biometrics Be Used for?	313
17.3	Classification of ECG Based Biometric Techniques	313
17.4	Comparison of Existing ECG Based Biometric Systems	316
17.5	Implementation of an ECG Biometric	318
17.6	Open Issues of ECG Based Biometrics Applications	323
17.7	Security Issues for ECG Based Biometric	327

17.8	Conclusions	328
	References	329
	The Authors	330
Part C Networking		
18	Peer-to-Peer Botnets	335
	<i>Ping Wang, Baber Aslam, and Cliff C. Zou</i>	
18.1	Introduction	335
18.2	Background on P2P Networks	336
18.3	P2P Botnet Construction	338
18.4	P2P Botnet C&C Mechanisms	339
18.5	Measuring P2P Botnets	342
18.6	Countermeasures	344
18.7	Related Work	347
18.8	Conclusion	348
	References	348
	The Authors	350
19	Security of Service Networks	351
	<i>Theo Dimitrakos, David Brossard, Pierre de Leusse, and Srijith K. Nair</i>	
19.1	An Infrastructure for the Service Oriented Enterprise	352
19.2	Secure Messaging and Application Gateways	354
19.3	Federated Identity Management Capability	358
19.4	Service-level Access Management Capability	361
19.5	Governance Framework	364
19.6	Bringing It All Together	367
19.7	Securing Business Operations in an SOA: Collaborative Engineering Example	372
19.8	Conclusion	378
	References	380
	The Authors	381
20	Network Traffic Analysis and SCADA Security	383
	<i>Abdun Naser Mahmood, Christopher Leckie, Jiankun Hu, Zahir Tari, and Mohammed Atiquzzaman</i>	
20.1	Fundamentals of Network Traffic Monitoring and Analysis	384
20.2	Methods for Collecting Traffic Measurements	386
20.3	Analyzing Traffic Mixtures	390
20.4	Case Study: AutoFocus	395
20.5	How Can We Apply Network Traffic Monitoring Techniques for SCADA System Security?	399
20.6	Conclusion	401
	References	402
	The Authors	404
21	Mobile Ad Hoc Network Routing	407
	<i>Melody Moh and Ji Li</i>	
21.1	Chapter Overview	407
21.2	One-Layer Reputation Systems for MANET Routing	408
21.3	Two-Layer Reputation Systems (with Trust)	412

21.4	Limitations of Reputation Systems in MANETs	417
21.5	Conclusion and Future Directions	419
	References	419
	The Authors	420
22	Security for Ad Hoc Networks	421
	<i>Nikos Komninos, Dimitrios D. Vergados, and Christos Douligeris</i>	
22.1	Security Issues in Ad Hoc Networks	421
22.2	Security Challenges in the Operational Layers of Ad Hoc Networks	424
22.3	Description of the Advanced Security Approach.....	425
22.4	Authentication: How to in an Advanced Security Approach	427
22.5	Experimental Results	428
22.6	Concluding Remarks	430
	References	431
	The Authors	432
23	Phishing Attacks and Countermeasures	433
	<i>Zulfikar Ramzan</i>	
23.1	Phishing Attacks: A Looming Problem	433
23.2	The Phishing Ecosystem	435
23.3	Phishing Techniques	439
23.4	Countermeasures.....	442
23.5	Summary and Conclusions	447
	References	447
	The Author	448
 Part D Optical Networking		
24	Chaos-Based Secure Optical Communications Using Semiconductor Lasers .	451
	<i>Alexandre Locquet</i>	
24.1	Basic Concepts in Chaos-Based Secure Communications	452
24.2	Chaotic Laser Systems	454
24.3	Optical Secure Communications Using Chaotic Lasers Diodes	460
24.4	Advantages and Disadvantages of the Different Laser-Diode-Based Cryptosystems	466
24.5	Perspectives in Optical Chaotic Communications	474
	References	475
	The Author	478
25	Chaos Applications in Optical Communications	479
	<i>Apostolos Argyris and Dimitris Syvridis</i>	
25.1	Securing Communications by Cryptography	480
25.2	Security in Optical Communications	481
25.3	Optical Chaos Generation	485
25.4	Synchronization of Optical Chaos Generators	491
25.5	Communication Systems Using Optical Chaos Generators	497
25.6	Transmission Systems Using Chaos Generators.....	499
25.7	Conclusions	507
	References	507
	The Authors	510

Part E Wireless Networking

26	Security in Wireless Sensor Networks	513
	<i>Kashif Kifayat, Madjid Merabti, Qi Shi, and David Llewellyn-Jones</i>	
26.1	Wireless Sensor Networks	514
26.2	Security in WSNs	515
26.3	Applications of WSNs	515
26.4	Communication Architecture of WSNs	518
26.5	Protocol Stack	519
26.6	Challenges in WSNs	520
26.7	Security Challenges in WSNs	522
26.8	Attacks on WSNs	527
26.9	Security in Mobile Sensor Networks	533
26.10	Key Management in WSNs	533
26.11	Key Management for Mobile Sensor Networks	544
26.12	Conclusion	545
	References	545
	The Authors	551
27	Secure Routing in Wireless Sensor Networks	553
	<i>Jamil Ibriq, Imad Mahgoub, and Mohammad Ilyas</i>	
27.1	WSN Model	554
27.2	Advantages of WSNs	554
27.3	WSN Constraints	555
27.4	Adversarial Model	555
27.5	Security Goals in WSNs	556
27.6	Routing Security Challenges in WSNs	559
27.7	Nonsecure Routing Protocols	559
27.8	Secure Routing Protocols in WSNs	563
27.9	Conclusion	573
	References	573
	The Authors	577
28	Security via Surveillance and Monitoring	579
	<i>Chih-fan Hsin</i>	
28.1	Motivation	579
28.2	Duty-Cycling that Maintains Monitoring Coverage	581
28.3	Task-Specific Design: Network Self-Monitoring	586
28.4	Conclusion	600
	References	600
	The Author	602
29	Security and Quality of Service in Wireless Networks	603
	<i>Konstantinos Birkos, Theofilos Chrysikos, Stavros Kotsopoulos, and Ioannis Maniatis</i>	
29.1	Security in Wireless Networks	604
29.2	Security over Wireless Communications and the Wireless Channel ...	609
29.3	Interoperability Scenarios	616
29.4	Conclusions	627
	References	627
	The Authors	629

Part F Software

30	Low-Level Software Security by Example	633
	<i>Úlfar Erlingsson, Yves Younan, and Frank Piessens</i>	
30.1	Background	633
30.2	A Selection of Low-Level Attacks on C Software	635
30.3	Defenses that Preserve High-Level Language Properties	645
30.4	Summary and Discussion	655
	References	656
	The Authors	658
31	Software Reverse Engineering	659
	<i>Teodoro Ciproso, Mark Stamp</i>	
31.1	Why Learn About Software Reverse Engineering?	660
31.2	Reverse Engineering in Software Development	660
31.3	Reverse Engineering in Software Security	662
31.4	Reversing and Patching Wintel Machine Code	663
31.5	Reversing and Patching Java Bytecode	668
31.6	Basic Antireversing Techniques	673
31.7	Applying Antireversing Techniques to Wintel Machine Code	674
31.8	Applying Antireversing Techniques to Java Bytecode	686
31.9	Conclusion	694
	References	694
	The Authors	696
32	Trusted Computing	697
	<i>Antonio Lioy and Gianluca Ramunno</i>	
32.1	Trust and Trusted Computer Systems	697
32.2	The TCG Trusted Platform Architecture	700
32.3	The Trusted Platform Module	703
32.4	Overview of the TCG Trusted Infrastructure Architecture	714
32.5	Conclusions	715
	References	715
	The Authors	717
33	Security via Trusted Communications	719
	<i>Zheng Yan</i>	
33.1	Definitions and Literature Background	720
33.2	Autonomic Trust Management Based on Trusted Computing Platform	727
33.3	Autonomic Trust Management Based on an Adaptive Trust Control Model	733
33.4	A Comprehensive Solution for Autonomic Trust Management	738
33.5	Further Discussion	743
33.6	Conclusions	743
	References	744
	The Author	746
34	Viruses and Malware	747
	<i>Eric Filiol</i>	
34.1	Computer Infections or Malware	748
34.2	Antiviral Defense: Fighting Against Viruses	760

34.3	Conclusion	768
	References	768
	The Author	769
35	Designing a Secure Programming Language	771
	<i>Thomas H. Austin</i>	
35.1	Code Injection	771
35.2	Buffer Overflow Attacks	775
35.3	Client-Side Programming: Playing in the Sandbox	777
35.4	Metaobject Protocols and Aspect-Oriented Programming	780
35.5	Conclusion	783
	References	783
	The Author	785
Part G Forensics and Legal Issues		
36	Fundamentals of Digital Forensic Evidence	789
	<i>Frederick B. Cohen</i>	
36.1	Introduction and Overview	790
36.2	Identification	791
36.3	Collection	792
36.4	Transportation	792
36.5	Storage	793
36.6	Analysis, Interpretation, and Attribution	793
36.7	Reconstruction	794
36.8	Presentation	795
36.9	Destruction	795
36.10	Make or Miss Faults	799
36.11	Accidental or Intentional Faults	799
36.12	False Positives and Negatives	800
36.13	Pre-Legal Records Retention and Disposition	800
36.14	First Filing	802
36.15	Notice	802
36.16	Preservation Orders	802
36.17	Disclosures and Productions	802
36.18	Depositions	803
36.19	Motions, Sanctions, and Admissibility	804
36.20	Pre-Trial	804
36.21	Testimony	805
36.22	Case Closed	805
36.23	Duties	806
36.24	Honesty, Integrity, and Due Care	806
36.25	Competence	806
36.26	Retention and Disposition	807
36.27	Other Resources	807
	References	807
	The Author	808
37	Multimedia Forensics for Detecting Forgeries	809
	<i>Shiguo Lian and Yan Zhang</i>	
37.1	Some Examples of Multimedia Forgeries	810

37.2	Functionalities of Multimedia Forensics	812
37.3	General Schemes for Forgery Detection	814
37.4	Forensic Methods for Forgery Detection	815
37.5	Unresolved Issues	825
37.6	Conclusions	826
	References	826
	The Authors	828
38	Technological and Legal Aspects of CIS	829
	<i>Peter Stavroulakis</i>	
38.1	Technological Aspects	830
38.2	Secure Wireless Systems	836
38.3	Legal Aspects of Secure Information Networks	838
38.4	An Emergency Telemedicine System/Olympic Games Application/CBRN Threats	844
38.5	Technology Convergence and Contribution	848
	References	848
	The Author	850
Index	851