

Inhalt

Materialien zum Buch	25
Geleitwort des Fachgutachters	27

1 Netzwerke im Überblick 29

1.1 Schichten	29
1.2 Datenrate, Durchsatz und Bandbreite	30
1.3 Pakete	31
1.4 Datagrammweiterleitung	33
1.5 Topologie	37
1.5.1 Traffic-Engineering	37
1.6 Routing-Schleifen	38
1.7 Überlast	40
1.8 Mehr über Pakete	41
1.9 LANs und Ethernet	42
1.10 IP – Internet Protocol	45
1.10.1 IP-Weiterleitung	49
1.10.2 Die Zukunft von IPv4	53
1.11 DNS	54
1.12 Transport	55
1.12.1 Muster der Traffic-Kommunikation	58
1.12.2 Content-Distribution Networks	60
1.13 Firewalls	61
1.14 Einige nützliche Dienstprogramme	63
1.15 IETF und OSI	65
1.16 Berkeley Unix	69
1.17 Epilog	70
1.18 Übungen	70

2 Ethernet-Grundlagen 75

- 2.1 Klassisches 10-Mbit/s-Ethernet** 76
 - 2.1.1 Ethernet-Paketformat 79
 - 2.1.2 Ethernet Multicast 80
 - 2.1.3 Interne Struktur von Ethernet-Adressen 81
 - 2.1.4 Die LAN-Schicht 82
 - 2.1.5 Slot-Zeit und Kollisionen 83
 - 2.1.6 Exponentieller Backoff-Algorithmus 86
 - 2.1.7 Capture-Effekt 88
 - 2.1.8 Hubs und Topologie 89
 - 2.1.9 Fehler 89
 - 2.1.10 CSMA-Persistenz 89
 - 2.1.11 Analyse des klassischen Ethernets 90
- 2.2 100 Mbit/s (Fast) Ethernet** 93
- 2.3 Gigabit-Ethernet** 95
- 2.4 Ethernet-Switches** 96
 - 2.4.1 Kosten für Switches 98
 - 2.4.2 Ethernet-Lernalgorithmus 98
- 2.5 Epilog** 101
- 2.6 Übungen** 102

3 Weiterführende Ethernet-Themen 107

- 3.1 Spanning-Tree-Algorithmus und Redundanz** 108
 - 3.1.1 Beispiel 1: Nur Switches 110
 - 3.1.2 Beispiel 2: Switches und Segmente 111
- 3.2 Virtuelles LAN (VLAN)** 114
 - 3.2.1 Switch-Hardware 116
- 3.3 TRILL und SPB** 119
- 3.4 Software-Defined Networking** 122
 - 3.4.1 OpenFlow-Switches 123
 - 3.4.2 Selbstlernende Switches in OpenFlow 125
 - 3.4.3 Weitere OpenFlow-Beispiele 127
- 3.5 Epilog** 132
- 3.6 Übungen** 132

4	Drahtlose LANs	137
4.1	Abenteuer im Funkland	137
4.1.1	Datenschutz	137
4.1.2	Kollisionen	138
4.1.3	Versteckte Teilnehmer (Hidden Nodes)	138
4.1.4	Bandbreite	139
4.1.5	Kosten	140
4.1.6	Mehrweginterferenz	141
4.1.7	Energieverbrauch	143
4.1.8	Kabelsalat	143
4.2	Wi-Fi	143
4.2.1	Wi-Fi und Kollisionen	147
4.2.2	Dynamische Geschwindigkeitsanpassung	152
4.2.3	Mehrere Spatial Streams	153
4.2.4	Zugangspunkte	156
4.2.5	Wi-Fi-Sicherheit	166
4.2.6	Wi-Fi Monitoring	176
4.2.7	Wi-Fi-Polling-Modus	177
4.2.8	MANETs	179
4.3	WiMAX und LTE	182
4.3.1	Uplink-Scheduling	184
4.3.2	Ranging	186
4.3.3	Network Entry	186
4.3.4	Mobility	187
4.4	Ortsfeste Drahtlosnetzwerke	188
4.4.1	Terrestrische Funknetzwerke	188
4.4.2	Satelliteninternet	189
4.5	Epilog	190
4.6	Übungen	191
5	Sonstige LAN-Technologien	195
5.1	Virtuelle private Netzwerke	195
5.2	Carrier-Ethernet	197
5.3	Token Ring	198
5.4	Virtuelle Verbindungen	200

5.5	Asynchronous Transfer Mode: ATM	204
5.5.1	ATM-Segmentierung und -Reassemblierung	206
5.6	Epilog	208
5.7	Übungen	208

6 Verbindungen 213

6.1	Kodierung und Frames	213
6.1.1	NRZ	214
6.1.2	NRZI	214
6.1.3	Manchester	215
6.1.4	4B/5B	215
6.1.5	Framing	217
6.2	Zeitmultiplexverfahren	220
6.2.1	T-Carrier-Leitungen	221
6.2.2	SONET	222
6.2.3	Optical Transport Network	225
6.2.4	Andere faseroptische Übertragungsarten	226
6.3	Epilog	227
6.4	Übungen	227

7 Pakete 229

7.1	Paketverzögerung	229
7.1.1	Beispiele für Verzögerungen	230
7.1.2	Bandbreite × Verzögerung	233
7.2	Schwankungen der Paketverzögerung	233
7.3	Paketgröße	234
7.3.1	Fehlerhäufigkeit und Paketgröße	236
7.3.2	Paketgröße und Echtzeit-Traffic	237
7.4	Fehlererkennung	237
7.4.1	Zyklische Redundanzprüfung: CRC	241
7.4.2	Fehlerkorrigierende Codes	243
7.5	Epilog	245
7.6	Übungen	245

8	Sliding Windows	251
8.1	Zuverlässige Datenübertragung: Stop-and-Wait	251
8.1.1	Paketverlust	252
8.1.2	Sorcerer's Apprentice Bug	254
8.1.3	Datenflusssteuerung	255
8.2	Die Sliding-Windows-Strategie	256
8.2.1	Bandbreite \times Verzögerung	258
8.2.2	Die Empfängerseite	259
8.2.3	Verlustwiederherstellung unter Sliding Windows	260
8.3	Lineare Flaschenhalse	261
8.3.1	Einfache Analyse für feste Fenstergröße	262
8.3.2	RTT-Berechnungen	266
8.3.3	Grafiken an der Überlastungsgrenze	268
8.3.4	Einfache paketbasierte Sliding-Windows-Implementierung	269
8.4	Epilog	271
8.5	Übungen	271
9	IP Version 4	277
9.1	Der IPv4-Header	279
9.2	Schnittstellen	282
9.2.1	Multihomed Hosts	283
9.3	Spezielle Adressen	284
9.3.1	Multicast-Adressen	286
9.4	Fragmentierung	287
9.5	Der klassenlose IP-Delivery-Algorithmus	290
9.5.1	Effizientes Lookup in der Weiterleitungstabelle	292
9.6	IPv4-Subnetze	294
9.6.1	Subnetz-Beispiel	298
9.6.2	Verbindungen zwischen Subnetzen	299
9.6.3	Subnetze versus Switching	301
9.7	Netzwerkadressübersetzung	302
9.7.1	Probleme mit NAT	305
9.7.2	Middleboxen	307
9.7.3	NAT-Traversal	308

9.8	Unnummerierte Schnittstellen	309
9.9	Mobile IP	311
9.9.1	IP-in-IP-Kapselung	312
9.10	Epilog	313
9.11	Übungen	313

10 IPv4-Begleitprotokolle 317

10.1	DNS	317
10.1.1	DNS-Resolver	320
10.1.2	nslookup und dig	326
10.1.3	Andere DNS-Einträge	332
10.1.4	DNS Cache Poisoning	334
10.1.5	DNS und CDNs	335
10.2	Address Resolution Protocol: ARP	336
10.2.1	ARP-Feinheiten	337
10.2.2	ARP-Sicherheit	339
10.2.3	ARP-Failover	340
10.2.4	Erkennung von Sniffern	340
10.2.5	ARP und Hosts mit mehreren Adressen	341
10.3	Dynamic Host Configuration Protocol (DHCP)	341
10.3.1	NAT, DHCP und das kleine Büro	342
10.3.2	DHCP und Router	343
10.4	Internet Control Message Protocol	343
10.4.1	Traceroute und Time Exceeded	347
10.4.2	Redirects	348
10.4.3	Router Solicitation	348
10.5	Epilog	349
10.6	Übungen	349

11 IPv6 351

11.1	Der IPv6-Header	352
11.2	IPv6-Adressen	353
11.2.1	Schnittstellenbezeichner	354

11.2.2	Link-local-Adressen	356
11.2.3	Anycast-Adressen	357
11.3	Netzwerkpräfixe	358
11.4	IPv6-Multicast	359
11.5	IPv6-Erweiterungsheader	360
11.5.1	Hop-by-Hop-Options-Header	361
11.5.2	Destination-Options-Header	361
11.5.3	Routing-Header	362
11.5.4	IPv6-Fragment-Header	362
11.5.5	Häufige Probleme mit dem Erweiterungs-Header	363
11.6	Nachbarschaftserkennung (Neighbor Discovery)	364
11.6.1	Router-Ermittlung (Router Discovery)	364
11.6.2	Präfix-Ermittlung (Prefix discovery)	365
11.6.3	Nachbarschaftsanfragen (Neighbor Solicitation)	367
11.6.4	Sicherheit und Nachbarschaftserkennung	368
11.7	Zuweisung von IPv6-Hostadressen	371
11.7.1	Erkennung doppelter Adressen	372
11.7.2	Zustandslose Autokonfiguration (Stateless Autoconfiguration, SLAAC)	373
11.7.3	DHCPv6	376
11.8	Epilog	378
11.9	Übungen	378
12	Weitere IPv6-Funktionen	381
12.1	Weltweit sichtbare Adressen	381
12.2	ICMPv6	382
12.2.1	Node Information Messages	383
12.3	IPv6-Subnetze	384
12.3.1	Subnetze und /64	385
12.4	IPv6 und IPv4 gemeinsam benutzen	386
12.5	IPv6-Beispiele ohne Router	392
12.5.1	ping6	392
12.5.2	TCP-Verbindungen mit Link-Local-Adressen	393
12.5.3	Manuelle Adresskonfiguration	393

12.6 IPv6-Konnektivität über Tunneling	395
12.6.1 IPv6-Firewalls	397
12.6.2 Einen Router einrichten	397
12.7 Konnektivität von IPv6 nach IPv4	400
12.8 Epilog	402
12.9 Übungen	402

13 Routing-Update-Algorithmen 405

13.1 Distanzvektor-Routing-Update-Algorithmus	406
13.1.1 Distanzvektor-Update-Regeln	407
13.2 Langsames Konvergenzproblem bei Distanzvektoren	413
13.2.1 Korrekturen für langsame Konvergenz	413
13.3 Minimierung der Streckenkosten	415
13.4 Schleifenfreie Distanzvektor-Algorithmen	418
13.4.1 DSDV	418
13.4.2 AODV	420
13.4.3 HWMP	424
13.4.4 EIGRP	425
13.5 Link-State-Routing-Update-Algorithmus	427
13.5.1 Shortest-Path-First-Algorithmus	429
13.6 Routing nach anderen Attributen	432
13.7 ECMP	434
13.8 Epilog	435
13.9 Übungen	436

14 IP-Routing im großen Maßstab 445

14.1 Classless Internet Domain Routing: CIDR	446
14.2 Hierarchisches Routing	449
14.3 Routing in früherer Zeit	450
14.4 Providerbasiertes Routing	451
14.4.1 Internet Exchange Points	453

14.4.2	CIDR (und wie man nicht ins Gefängnis kommt)	454
14.4.3	Hierarchisches Routing über Provider	455
14.4.4	IP-Geolokalisierung	457
14.5	Geografisches Routing	458
14.6	Epilog	459
14.7	Übungen	459
15	Border Gateway Protocol (BGP)	465
15.1	AS-Pfade	467
15.2	AS-Pfade und Routenaggregation	469
15.3	Transit-Traffic	471
15.4	BGP-Filterung und Routing-Policies	471
15.5	BGP-Tabellengröße	474
15.6	BGP-Pfadattribute	475
15.6.1	NEXT_HOP	476
15.6.2	LOCAL_PREF	476
15.6.3	MULTI_EXIT_DISC	476
15.6.4	COMMUNITY	479
15.7	BGP und Traffic-Engineering	480
15.7.1	MED-Werte und Traffic-Engineering	483
15.8	BGP und Anycast	484
15.9	BGP für internes Routing	485
15.10	BGP-Beziehungen	486
15.10.1	BGP-No-Valley-Theorem	491
15.11	Beispiele für BGP-Instabilität	492
15.12	BGP-Sicherheit und Route Registrys	494
15.12.1	IRR-Abfragen	496
15.12.2	RPKI	498
15.13	Epilog	500
15.14	Übungen	500

16 UDP-Übertragung 503

- 16.1 User Datagram Protocol – UDP** 503
 - 16.1.1 QUIC 505
 - 16.1.2 DCCP 506
 - 16.1.3 Simplex-Talk über UDP 507
 - 16.1.4 netcat 517
 - 16.1.5 Binärdaten 517
- 16.2 Trivial File Transport Protocol, TFTP** 520
- 16.3 Grundlegende Übertragungsprobleme** 523
 - 16.3.1 Alte, doppelte Pakete 524
 - 16.3.2 Verlorenes abschließendes ACK 526
 - 16.3.3 Doppelte Verbindungsanforderung 529
 - 16.3.4 Reboots 530
- 16.4 Weitere Anmerkungen zu TFTP** 531
 - 16.4.1 TFTP und der Zauberlehrling 531
 - 16.4.2 TFTP-Zustände 531
 - 16.4.3 Durchsatz bei TFTP 533
- 16.5 Remote Procedure Call (RPC)** 534
 - 16.5.1 Network File System 536
 - 16.5.2 Sun RPC 536
 - 16.5.3 Seriale Ausführung 538
 - 16.5.4 Verfeinerungen von RPC 538
- 16.6 Epilog** 539
- 16.7 Übungen** 539

17 Grundlagen des TCP-Transports 545

- 17.1 Das Ende-zu-Ende-Prinzip** 547
- 17.2 TCP-Header** 547
- 17.3 Aufbau einer TCP-Verbindung** 549
- 17.4 TCP und Wireshark** 555
- 17.5 TCP-Offloading** 557
- 17.6 TCP-Simplex-Talk** 558
 - 17.6.1 Der TCP-Server 558
 - 17.6.2 Der TCP-Client 561

17.7 TCP und bind()	563
17.7.1 Noch einmal netcat	564
17.8 TCP-Zustandsdiagramm	565
17.8.1 Eine Verbindung beenden	567
17.8.2 Close() aufrufen	569
17.9 Epilog	572
17.10 Übungen	572
18 TCP – Probleme und Alternativen	577
<hr/>	
18.1 Alte Duplikate bei TCP	577
18.2 TIMEWAIT	578
18.3 Der dreifache Handshake – erneut betrachtet	580
18.4 Anomale TCP-Szenarien	583
18.5 Schnelleres Öffnen von TCP-Verbindungen	584
18.6 Path MTU Discovery	587
18.7 Sliding Windows bei TCP	587
18.8 Verzögerte ACKs bei TCP	588
18.9 Nagle-Algorithmus	589
18.10 Flusststeuerung bei TCP	590
18.11 Silly-Window-Syndrom	591
18.12 Zeitüberschreitung und Neuübertragung bei TCP	592
18.13 KeepAlive	594
18.14 TCP-Timer	594
18.15 Varianten und Alternativen	595
18.15.1 MPTCP	595
18.15.2 SCTP	597
18.15.3 DCCP	599
18.15.4 Ein neuerlicher Blick auf QUIC	600
18.16 Epilog	608
18.17 Übungen	608

19 TCP Reno und Überlastmanagement 611

19.1 Grundlagen des TCP-Überlastmanagements 612

 19.1.1 Der einigermaßen stationäre Zustand 615

19.2 Slow Start 618

 19.2.1 Per-ACK-Antworten 620

 19.2.2 Slow Start Threshold 620

 19.2.3 Beispiel: Slow Start bei mehreren Paketen 622

 19.2.4 Zusammenfassung des bisher Gelernten 623

 19.2.5 Der Anfangswert von cwnd 624

19.3 TCP Tahoe und Fast-Retransmit 624

19.4 TCP Reno und Fast-Recovery 626

19.5 TCP NewReno 630

19.6 Selektive Bestätigungen (SACK) 632

19.7 TCP und Auslastung der Flaschen Halsverbindung 633

 19.7.1 TCP-Warteschlangengrößen 636

19.8 Verluste einzelner Pakete 638

19.9 Annahmen zu TCP und Skalierbarkeit 639

19.10 TCP-Parameter 640

19.11 Epilog 641

19.12 Übungen 641

20 TCP-Dynamik 647

20.1 Ein erster Blick auf das Queuing 647

 20.1.1 Priority Queuing 648

20.2 Flaschen Halsverbindungen mit konkurrierendem Datenverkehr 649

 20.2.1 Beispiel 1: Linearer Flaschenhals 649

 20.2.2 Beispiel 2: Router-Wettbewerb 649

 20.2.3 Beispiel 3: Wettbewerb und Warteschlangenauslastung 651

 20.2.4 Beispiel 4: Querverkehr und RTT-Schwankungen 655

 20.2.5 Beispiel 5: Veränderliche Flaschenhäse 657

 20.2.6 Paketpaare 658

20.3 TCP Reno – Fairness mit synchronisierten Verlusten 659

 20.3.1 Beispiel 2: Schnellerer additiver Zuwachs 662

20.3.2	Beispiel 3: Längere RTT	663
20.3.3	Beeinflussung der RTT bei TCP Reno	665
20.3.4	Hypothese der synchronen Verluste	666
20.3.5	Verlust-Synchronisierung	667
20.3.6	Extreme RTT-Unterschiede	668
20.4	Epilog	669
20.5	Übungen	669

21 Weitere TCP-Dynamiken 675

21.1	Begriffe der Fairness	675
21.1.1	Max-Min-Fairness	675
21.1.2	Proportionale Fairness	677
21.2	TCP-Reno-Verlustrate und cwnd	677
21.2.1	Ungleichmäßige Sägezähne	679
21.2.2	Nicht synchronisierte TCP-Verlustereignisse	679
21.3	TCP-Freundlichkeit	680
21.3.1	TFRC	681
21.3.2	RTP	682
21.3.3	DCCP-Überlaststeuerung	683
21.4	Noch einmal AIMD	684
21.4.1	AIMD und Konvergenz zur Fairness	686
21.5	Aktives Warteschlangenmanagement	686
21.5.1	Bufferbloat	687
21.5.2	DECbit	688
21.5.3	Explicit Congestion Notification (ECN)	689
21.5.4	RED	691
21.5.5	ADT	692
21.5.6	CoDel	693
21.6	Das TCP-Problem der hohen Bandbreiten	694
21.7	Das Problem der verlustbehafteten Verbindungen	696
21.8	Das Problem der Satelliten-TCP-Verbindungen	697
21.9	Epilog	697
21.10	Übungen	698

22 Queuing und Scheduling 705

- 22.1 Queuing und Echtzeitdatenverkehr** 706
- 22.2 Traffic-Management** 707
- 22.3 Priority Queuing** 708
- 22.4 Warteschlangenverfahren** 708
- 22.5 Fair Queuing** 710
 - 22.5.1 Weighted Fair Queuing 711
 - 22.5.2 Virtuelle Fertigstellungszeiten 712
 - 22.5.3 Bitweises Round-Robin-Verfahren 716
 - 22.5.4 Das GPS-Modell 719
 - 22.5.5 Deficit Round Robin 728
 - 22.5.6 Stochastisches Fair Queuing 729
- 22.6 Anwendungen von Fair Queuing** 730
 - 22.6.1 Fair Queuing und Bufferbloat 731
- 22.7 Hierarchisches Queuing** 733
 - 22.7.1 Generisches hierarchisches Queuing 734
 - 22.7.2 Hierarchische Beispiele 735
- 22.8 Hierarchical Weighted Fair Queuing** 737
 - 22.8.1 Algorithmus für Hierarchical Weighted Fair Queuing 740
- 22.9 Epilog** 744
- 22.10 Übungen** 745

23 Token-Bucket 749

- 23.1 Token-Bucket – Definition** 750
- 23.2 Token-Bucket – Beispiele** 753
- 23.3 Mehrere Token-Buckets** 754
- 23.4 GCRA** 755
 - 23.4.1 Anwendungen von Token-Bucket 756
- 23.5 Gewährleistung der VoIP-Bandbreite** 757
- 23.6 Verzögerung begrenzen** 758
 - 23.6.1 Auslastung der Token-Bucket-Warteschlange 759
- 23.7 Token-Bucket durch einen Router** 760

23.8	Token-Bucket durch mehrere Router	761
23.9	Verzögerungsbedingungen	762
23.9.1	Hierarchischer Token-Bucket	762
23.9.2	Kombinationen aus Fair Queuing und Token-Bucket	764
23.10	CBQ	765
23.11	Linux HTB	765
23.12	Parekh-Gallager Theorem	767
23.13	Epilog	768
23.14	Übungen	768

24 Quality of Service 773

24.1	Netzneutralität	775
24.2	Wo die wilden Warteschlangen wohnen	775
24.3	Echtzeit-Datenverkehr	776
24.3.1	Wiedergabepuffer	777
24.3.2	Videostreaming	779
24.3.3	UDP und Echtzeitdatenverkehr	780
24.4	Integrated Services/RSVP	780
24.5	Globales IP-Multicast	781
24.6	RSVP	788
24.6.1	Eine CDN-basierte Alternative zu IntServ	791
24.7	Differentiated Services	794
24.7.1	Expedited Forwarding	796
24.7.2	Assured Forwarding	799
24.8	RED with In and Out	801
24.9	NSIS	801
24.10	Comcast-System zu Überlaststeuerung	802
24.11	Real-time Transport Protocol (RTP)	804
24.11.1	RTP-Mixer	805
24.11.2	RTP-Paketformat	806
24.11.3	RTP Control Protocol	808
24.11.4	RTP und VoIP	809

24.12 Multi-Protocol Label Switching (MPLS) 810
24.13 Epilog 814
24.14 Übungen 814

25 Netzwerkverwaltung und SNMP 817

25.1 Netzwerkarchitektur 820
25.2 SNMP-Grundlagen 820
 25.2.1 SNMP-Versionen 822
25.3 Namen und OIDs unter SNMP 823
25.4 MIBs 825
25.5 SNMPv1-Datentypen 827
25.6 ASN.1-Syntax und SNMP 828
25.7 SNMP-Tabellen 829
25.8 SNMP-Operationen 835
 25.8.1 Get() mit mehreren Attributen 839
 25.8.2 Set() 840
25.9 MIB-Browsing 841
25.10 MIB-2 842
 25.10.1 Die system-Gruppe 843
 25.10.2 Tabellendefinitionen und die interfaces-Gruppe 844
 25.10.3 Die ip-Gruppe 850
 25.10.4 Die icmp-Gruppe 852
 25.10.5 Die tcp-Gruppe 852
 25.10.6 Die udp-Gruppe 853
 25.10.7 Die snmp-Gruppe 853
25.11 SNMPv1-Communitys und -Sicherheit 853
25.12 SNMP und die ASN.1-Kodierung 855
 25.12.1 Primitive Typen 856
 25.12.2 Zusammengesetzte Typen 858
25.13 Übungen 859

26 Die SNMP-Versionen 2 und 3	863
26.1 SNMPv2	863
26.1.1 SMI und Datentypen von SNMPv2	863
26.1.2 SNMPv2-Get-Semantik	864
26.1.3 SNMPv2-GetBulk()	864
26.1.4 SNMPv2-Indizes	866
26.1.5 TestAndIncr	867
26.1.6 Table Augmentation	868
26.1.7 MIB-Veränderungen in SNMPv2	870
26.1.8 sysORTable	870
26.1.9 IF-MIB und ifXTable	871
26.1.10 ETHERLIKE-MIB	872
26.1.11 BRIDGE-MIB	873
26.1.12 IP-MIB und IP-Forward-MIB	874
26.1.13 TCP-MIB	878
26.2 Erstellung von Tabellenzeilen	879
26.2.1 RMON	880
26.2.2 SNMPv2 RowStatus	888
26.2.3 PING-MIB	889
26.3 SNMPv3	890
26.3.1 What Could Possibly Go Wrong?	891
26.3.2 Kryptografische Grundlagen	892
26.3.3 SNMPv3-Engines	893
26.3.4 Authentifizierung von Nachrichten	894
26.3.5 Passwörter und Schlüssel	895
26.3.6 Signieren von Nachrichten	896
26.3.7 Veränderung des Schlüssels	896
26.3.8 Zusätzliche Nutzer anlegen	897
26.3.9 VACM für SNMPv3	898
26.4 Übungen	905
27 Sicherheit	907
27.1 Einbruch mit Ausführung von Code	909
27.1.1 Der Morris-Wurm	910
27.1.2 Christmas-Day-Attacke	910

27.2 Stapelüberlauf	911
27.2.1 Return to libc	912
27.2.2 Ein konkretes Beispiel für einen Stapelüberlauf	913
27.2.3 Schutzmaßnahmen gegen Pufferüberläufe	920
27.3 Heap-Überlauf	923
27.3.1 Eine Heap-Sicherheitslücke unter Linux	924
27.3.2 Eine Heap-Sicherheitslücke in Zusammenhang mit JPEG	926
27.3.3 Cross-Site-Scripting (XSS)	928
27.3.4 SQL-Injektion	929
27.4 Network Intrusion Detection	930
27.5 Ziele der Kryptografie	932
27.6 Sichere Hashes	934
27.6.1 Sichere Hashes und Authentifizierung	936
27.6.2 Passwort-Hashes	938
27.6.3 CHAP	939
27.6.4 SCRAM	939
27.7 Verschlüsselung mit gemeinsamem Schlüssel	940
27.7.1 Sitzungsschlüssel	941
27.7.2 Blockverschlüsselung	942
27.7.3 Verschlüsselungsmodi	945
27.7.4 Stromverschlüsselung	946
27.7.5 Auf Blockverschlüsselung basierende Stromverschlüsselungs- verfahren	948
27.7.6 Verschlüsselung und Authentifizierung	949
27.7.7 Versagen der WEP-Verschlüsselung für Wi-Fi	950
27.8 Diffie-Hellman-Merkle-Schlüsselaustausch	954
27.8.1 Schnelle Arithmetik	956
27.8.2 Simultaneous Authentication of Equals	956
27.9 Übungen	959

28 Verschlüsselung mit öffentlichem Schlüssel 963

28.1 RSA	963
28.1.1 RSA und digitale Signaturen	965
28.1.2 RSA-Schlüssel faktorisieren	966
28.2 Vorwärts gerichtete Geheimhaltung	967
28.3 Vertrauen und der Mann in der Mitte	969

28.4	Ende-zu-Ende-Verschlüsselung	970
28.5	SSH und TLS	971
28.5.1	SSH	972
28.5.2	TLS	976
28.5.3	Ein TLS-Programmierbeispiel	990
28.6	IPsec	998
28.6.1	Sicherheitsverbindungen (Security Associations)	1000
28.7	DNSSEC	1002
28.7.1	DNSSEC verwenden	1009
28.7.2	DNS-based Authentication of Named Entities	1011
28.7.3	Warum ist DNSSEC nicht weiter verbreitet?	1013
28.7.4	DNS over HTTPS	1015
28.8	Beispiele mit RSA-Schlüssel	1016
28.9	Übungen	1020
	Bibliografie	1023
	Index	1033

Materialien zum Buch


Auf der Webseite zu diesem Buch stehen folgende Materialien für Sie zum Download bereit:

- ▶ **Beispieldateien**
- ▶ **Musterlösungen zu den markierten Aufgaben**

Gehen Sie auf www.rheinwerk-verlag.de/5561. Klicken Sie auf den Reiter MATERIALIEN. Sie sehen die herunterladbaren Dateien samt einer Kurzbeschreibung des Dateiinhalts. Klicken Sie auf den Button HERUNTERLADEN, um den Download zu starten. Je nach Größe der Datei (und Ihrer Internetverbindung) kann es einige Zeit dauern, bis der Download abgeschlossen ist.

Die amerikanische Originalausgabe finden Sie unter <http://intronetworks.cs.luc.edu>

Der vollständige Text der RFCs können unter <https://www.rfc-editor.org> eingesehen werden.

Diese Leseprobe haben Sie beim
 edv-buchversand.de heruntergeladen.
Das Buch können Sie online in unserem
Shop bestellen.

[Hier zum Shop](#)