

Index

Page numbers printed in **bold face** indicate the location in the book where the term is defined, or where the primary discussion of it is located.

- * (host), 177, 178, 180, 181, 184, 185
- *.ATT.COM (host), 31
- .. (directory), 65, 69, 86
- ... (file), 305, 306
- .NET, *see* Microsoft, .NET
- .gift (file), 123
- .htaccess (file), 85
- .pdf (file), 79
- .rhosts (file), 44, 56, 59, 60, 156, 168
- .s.c (program), 306
- .shosts (file), 156
- .ssh (directory), 105
- .ssh/authorized_keys2 (file), 156
- .ssh/id_dsa (file), 156
- .ssh/id_dsa.pub (file), 156
- \$HOME/.rhosts (file), 60
- /usr/lib/term/.s (directory), 426
- /bin (directory), 290, 293
- /bin/sh (file), 166
- /ches/index.html (file), 78
- /dev (directory), 295
- /dev/kmem (file), 43
- /dev/tty (file), 163, 293
- /etc (directory), 268
- /etc/group (file), 163, 268
- /etc/hosts (file), 295
- /etc/hosts.equiv (file), 59, 60
- /etc/inetd.conf (file), 122, 165, 266, 267, 269
- /etc/motd (file), 268, 294, 303, 309
- /etc/passwd (file), 50, 56, 57, 60, 96, 98, 163, 168, 268
- /etc/resolv.conf (file), 163, 201
- /home/rubin/www-etc/.htpasswd (directory), 85
- /lib (directory), 163
- /lib/rld (file), 163
- /private/32-frobozz#\$ (file), 57
- /usr/apache (directory), 165
- /usr/ftp (directory), 60
- /usr/lib (directory), 163, 305, 309
- /usr/lib (file), 305
- /usr/lib/awk/ (directory), 305
- /usr/lib/lbb.aa (file), 309
- /usr/lib/libc.so.1 (file), 163
- /usr/lib/libm.so (file), 163
- /usr/lib/sendmail (file), 168, 302, 310
- /usr/lib/term/.s (directory), 298
- /usr/local/boot (directory), 52
- /usr/spool/uucppublic (directory), 60
- /usr/var/tmp (directory), 305, 306
- /var/spool/mqueue (directory), 43
- 1.2.3.4 (host), 189, 190
- 10.11.12.13 (host), 190
- 127.0.0.1 (host), 71
- 192.20.225.4 (host), 32
- 2600 Magazine, 349
- 4.225.20.192.IN-ADDR.ARPA (host), 32
- 5.6.7.8 (host), 189, 190
- 5.7.6.8 (host), 189
- 6over4 (program), 37
- 6to4 (program), 37
- 7ESS.MYMEGACORP.COM (host), 33
- 802.11, 38, 105, 242



- WEP, *see* WEP
- A1 (host), 320
- A2 (host), 320
- access control lists, **48**
- ACM (Association for Computing Machinery), 353
- ActiveX, 264
 - filtering with a proxy, 202
 - uses digital signatures, 270
 - Web browser controls for, 84
- Address Resolution Protocol, *see* ARP
- address-based authentication, *see* authentication, address-based
- address-spoofing, *see* attacks, address-spoofing
- adjunct password file, *see* passwords, file, shadow
- Adleman, Leonard, 343
- administration, 296
- Administrator* (account), 123, 210
- ADMINNET (host), 184
- Adobe
 - Acrobat Reader, 79
- adrian* (account), 288, 289
- Advanced Encryption Standard, *see* AES
- Advanced Research Projects Agency, *see* DARPA
- adware, **69**
- AES (Advanced Encryption Standard), 40, **337–339**
 - modes of operation, 338
- AFS (Andrew File System), 52
 - authentication, 52
- AH (Authentication Header), 36, 318, 319
- AIM, *see* AOL, Instant Messenger
- Airsnort* (program), 39
- AIX
 - setuid programs on, 124
- Alderson drive, 233
- alligators, 65
- Allman, Eric, 158
- AllowUsers, 156
- America Online, *see* AOL
- Andrew File System, *see* AFS
- ANI, 260
- anonymous* (account), 55
- anonymous certificates, *see* certificates, anonymous
- anonymous FTP, *see* FTP, anonymous
- AntiSniff, 159
- anycast addresses, **35**
- AOL
 - Instant Messenger
 - UNIX client, 46
 - connects to master servers, 45
 - passwords sniffed by *dsniff*, 129
- AP news, 309
- Apache Web server, 270
 - jailing, 165–167
 - on medium-security hosts, 255
 - restricting file access, 85
 - shared libraries and, 165
 - suexec* and, 167
 - version 2.0, 165
- APOP, *see* POP3, APOP authentication
- applets, **81**
- arms races, **xiii**
 - snort* and attack packets, 283
 - between virus writers and detection software, 107, 331
 - cryptographic key length, 338
 - for acquiring *root*, 125
 - password pickers vs. password guessers, 95
 - spoofers vs. packet telescope sizes and locations, 117
 - spotting DOS attack packets, 111
- ARMY.COM (host), 78
- ARP (Address Resolution Protocol), **22**
 - replaced by ND in IPv6, 36
 - spoofing, **22**, 34, 160
 - man-in-the-middle attacks, 118
- ARPA, **19**
- ARPANET, 19
- AS (Autonomous System), 30
 - path, 31
- ASCII
 - 7-bit in SMTP, 41
 - in FTP transfers, 55
 - routine use for safe messages, 205
 - used by SIP, 47
- ASN.1, **62**
 - security problems with, 62
 - used by H.323, 47

- used by LDAP, 65
- used in MIBs, 62
- Association for Computing Machinery, *see* ACM
- assurance requirements, 12, 102
- astronauts, 67
- asymmetric cryptosystems, *see* cryptography, public key
- asymmetric routing, *see* routing, asymmetric
- Asynchronous Transfer Mode, *see* ATM
- AT&T Corp., 99, 248
 - divestiture, 11
 - net 12.0.0.0/8, 116
 - phone book, 97
- AT&T Labs
 - VPN, 244
- ATM (Asynchronous Transfer Mode), 20, 182
- ATT.ORG (host), 78
- attachments, 205
- attacks, **95–118**
 - active, 59, **117–118**, 337
 - address scanning, 33
 - address-spoofing, 23, 27, 48, 104, 149, 161, 179, 183
 - ARP-spoofing, 22, 34, 118
 - back doors, 100–103
 - in shared libraries, 164
 - birthday, 337, 346
 - bogus NIS backup servers, 50
 - change file timestamps, 63
 - chosen-plaintext, 336
 - code book, 339
 - connection laundering, 8
 - cryptographic, 313, 336
 - cut-and-paste, 337
 - denial-of-service, *see* DOS
 - dictionary, 50, 53, 60, 62, 96, 287
 - hacking tools for, 129
 - on POP3/APOP, 204
 - distributed denial-of-service, *see* DDoS
 - DNS cache contamination, 32
 - DNS spoofing, 330
 - DNS zone transfers, 31
 - dumpster diving, **132**
 - executable files in FTP area, 65
 - exhaustive search, 336, 338
 - exponential, **106–107**
 - fetching /etc/passwd, 98
 - FMS, 39
 - forged signatures, 327
 - hiding, **126–127**
 - inside, 14, 186, 187
 - IP fragmentation, 21
 - IP source routing, 29, 179
 - IP spoofing, 72
 - Kerberos authenticators, 317
 - known-plaintext, 336
 - laundering connections, 299
 - mail address-spoofing, 99
 - man-in-the-middle, 337, 344
 - DHCP subject to, 34
 - MBone packets through a packet filter, 67
 - name server, 149
 - name-spoofing, 32, 59
 - network scans, 33
 - on Kerberos' initial ticket, 317
 - on smart cards, 147
 - oracle, 337
 - passive eavesdropping, 29, 128, 337
 - password logging, 128
 - power attacks, 147
 - practical cryptanalysis, 336
 - protocol holes, 104
 - race, 144
 - replay, 149, 314, 326, 337
 - during clock skew, 144
 - foiled by different challenge, 148
 - IVs prevent, 340
 - Kerberos authenticators, 317
 - on Web servers, 76
 - set back time, 64
 - routing, 28, 29
 - rubber hose, 336
 - Smurf, 110
 - directed broadcasts and, 71
 - use directed broadcasts, 121
 - sniffing, xiii, 310
 - social engineering, 132
 - subversion by route confusion, 183
 - subverting routing with ICMP Redirect, 27
 - SYN flood, xiii
 - SYN packets, 109
 - TCP hijacking, xiii
 - TCP sequence number, 23, 29, 104, 118

- temporary visitor account, 99
- through *guest* account, 12
- time-spoofing, 63–64, 337
- timing attacks, 147
- traffic analysis, 318
- Trojan horse, 52, 57, 58, 63, 100, 128
- using CGI scripts, 166
- using `PATH`, 123
- version-rollback, 45
- via trusted hosts, 60
- weak random number generation
 - NFS, 51
- weakest link, 102
- auditing
 - concealing from, 63
 - nmap* has limited value for, 130
 - Orange Book and, 11
 - sensitive hosts, 8
 - with *netstat*, 267
- authentication, **137–151**
 - address-based
 - ssh* and, 158
 - address-based, 23, 32, 60, 70, **149**
 - fails, 28
 - based on internal and external DNS, 198
 - based on source address, 149
 - bidirectional, 315
 - BSD, **59**
 - by name, 51, 59
 - challenge/response, 145–147, 317, 342, 346
 - X11, 71
 - cryptographic, 64, 103, 137, 149–150, 313
 - database, 138, 144
 - failures, 103–104
 - for proxy use, 188
 - handheld authenticators, 138
 - host-to-host, 149–150
 - Kerberos, 11, 313–317
 - in AFS, 52
 - Lamport’s algorithm, **146–147**
 - magic cookie, 71
 - name-based, 32, **149**
 - network-based, 149
 - NFS, 51, 52
 - not provided by UDP, 27
 - one-factor
 - in *ssh*, 154–156
 - one-time passwords
 - racers, 104
 - OSPF, 29
 - other, 137
 - passwords
 - machine-chosen, 139
 - user-chosen, 138
 - philosophy, 99–100
 - pki, 150–151
 - Radius, **148**
 - RPC, 48
 - SASL, **149**
 - server, 146
 - SNMP, 326
 - something you are, **137**
 - something you have, **137**, 146
 - something you know, **137**, 138, 146
 - tickets, 316
 - time-based, 64, 144, 342
 - tokens, 260
 - two-factor, 137
 - in *ssh*, 157
 - upper management, 138
 - X11, 103
- Authentication Header, *see* AH
- authentication races, **104**
- authenticator, **314**, 316
 - handheld, 14, 59, 105, **144**, 146, 149
- authorization, 48, **137**
- `authorized_keys` (file), 105
- automatic teller machine, 146
- Autonomous System, *see* AS
- awk* (program), 219
- B (host), 320
- b* (account), 290, 291
- B1 (host), 320
- B2 (host), 320
- back doors, 11, 100–103
- backscatter, **116–117**
- backup
 - day-zero, 270, **273**
 - DNS servers, 31
 - encrypting tapes, 16
 - network links, 183
 - NIS servers, 50

- of safe hosts, 273
- bansho, 4
- Basic Authentication, 85
- basket, 279
- battlements, 11
- beferdd* (account), 291
- Beijing, perimeter failure near, 5
- Bell Laboratories
 - Plan 9 project, *see* Plan 9
 - XUNET project, 301
- BELL-LABS (host), 78
- BELLDASHLABS (host), 78
- Bellovin
 - Daniel, 2
 - Rebecca, 2
 - Sam, 2
 - Steve, 287, 295
 - Sylvia, 2
- belt-and-suspenders, **4, 255**
- Berferd, 125, 287–299
 - mother of, 299
 - origin of, 298–299
- berferd* (account), 78, 291, 295
- Berkeley packet filter, *see* BPF
- BGP (Border Gateway Protocol), **30–31**
 - diverting packet flows with, 30
 - filtering announcements, 30
 - filtering out bad packets with, 113, 115
 - MD5 authentication, 30
 - problems with fixing, 30
 - under increasing attack, 331
- bibtex* (program), 355
- big nose, 167
- big words
 - Alyce, 139
 - anathema, 11
 - bansho, 4
 - chimera, 9
 - concomitant, 102
 - cyclotrimethylenetrinitramine, 207
 - demimonde, 56
 - deprecated, 120, 287
 - ecchymosis, 139
 - helminthiasis, 206
 - immortelle, 139
 - indicia, 280
 - metastasis, 127
 - monoculture, 112
 - monostely, 139
 - neologism, 192, 288
 - obviate, 183
 - pedagogy, 197
 - postern, 11
 - provenance, xvii, 103
 - sanguine, 12
 - tautological, 85
- bin* (account), 60, 125, 297
- bin* (directory), 60, 123, 166
- bind*
 - graph patch rates, 276
- bind* (account), 170
- bind* (program), 31, 275, 276
- bind, 43
- biometrics, **147–148**, 260
- birds
 - African swallow, 239
 - European swallow, 239
 - pigeon, 235
- birds of a feather, *see* BoF
- birthday paradox, **347**
- bitrot, 312
- black box testing, 230
- black-bag jobs, 8
- black-holed, **249**
- blaster, atom, 119
- Bloom filter, 113
- BoF (birds of a feather), 353
- boofhead, 53
- BOOTP, **33–34**
- Border Gateway Protocol, *see* BGP
- Borisov, Nikita, 38
- botnets, **117**
- bots, **117**
- bounce attacks, *ftp*, 55
- BPF (Berkeley packet filter), 214
- branch offices
 - VPNs and, 237
- BrickHouse* (program), 220
- bro* (program), 214, 282
- broadcast
 - DHCP, 33
 - relayed elsewhere, 34
 - directed, 71
 - disable forwarding of, 21

- scanning for hosts with, 121
 - DOS using the small services, 71
 - format of, 21
 - in IPv6, 36
 - monitoring at a firewall, 219
 - multicast and, 36
 - storms, 72
 - TFTP router configuration with, 53
 - X11 XDMCP messages, 71
- brute force, *see* attacks, exhaustive search
- BSD, 255
 - authentication, **59**
 - often defaults to all services turned off, 255
 - ps* command, 292
 - uses client pull, 274
- BSD/OS
 - setuid programs on, 124
- BSDI, 261
 - BSD/OS, 72
- buffer overruns, *see* stack-smashing
- bugs, **100–103**
 - in critical systems, 16
 - in *fpd*, 56
 - in MIME processing, 43
 - in WWW file pointers, 65
 - old ones aren't fixed, 13
 - possible, in router, 9
 - programs are assumed to have, 5, 11
 - source routing, 183
- Bugtraq, 82, 83, 122, **350**
- bugtraq* (account), 416
- bulkheads, 253
- byte code, **81**

- C, 86
- C (host), 320
- C++, 81
- CA (Certificate Authority), **150**
 - SSL and root, 325
 - X.509 uses, 326
- cache, 316, 317
- caller ID, 260
- CAST, 327
- CBC (Cipher Block Chaining), 339, 340
- CCS (Computers and Communication Security), 353

- CD-ROM, 299
- CERT (Computer Emergency Response Team), **xiii**, 184, 292, 309, 311, 350
 - Advisories, **350**
 - CA-00:11, 108
 - CA-1992-11, 164
 - CA-1992-15, 6
 - CA-1995-03a, 15
 - CA-1997-22, 170
 - CA-1997-27, 55
 - CA-1998-05, 170, 275
 - CA-1998-07, 15
 - CA-1999-14, 170
 - CA-1999-15, 15, 61
 - CA-2000-02, 83
 - CA-2001-02, 170
 - CA-2001-04, 80
 - CA-2001-09, 24
 - CA-2001-26, 83
 - CA-2002-03, 62
 - CA-2002-06, 148
 - CA-2002-18, 275
 - CA-2002-23, 15
 - CA-2002-24, 275
 - CA-2002-27, 15, 117, 171
 - CA-91:04, 99
 - CA-95:01, 24
 - CA-95:13, 158
 - CA-96:03, 262
 - CA-96:06, 167
 - CA-96:21, 24
 - CA-96:26, 108
 - CA-97:24, 167
 - CA-97:28, 21
 - Incident Notes
 - IN-2000-02, 58
 - Vendor-Initiated Bulletins
 - VB-95:08, 71
 - Vulnerability Notes
 - VN-98:06, 83
 - VU#32650 - DOS, 58
 - VU#40327, 61
 - VU#596827, 61
 - VU#846832, 164
- Certificate Authority, *see* CA
- certificates, **345**
 - PGP, 327

- Web access, 77
- CFB (Cipher Feedback), 341
- CGI (Common Gateway Interface), 77
- CGI scripts, **86**, 87, **166**
 - chroot and, 165, 167
 - creating with anonymous FTP access, 65
 - easier to write than X11 programs, 91
 - hacking targets, 167
 - more dangerous than Java, 80
 - need wrappers, 86
 - replaced with Java applets, 82
 - shell escape characters and, 86
- CGI wrappers, 86, **166–167**
- CGIWrap* (program), 165, 167
- challenge/response, *see* authentication, challenge/response
- Chapin, A. Lyman, 28
- Chapman, Brent, 177, 199, 201, 232
- chargen* (program), 71
- chargen*, 72
- checksum
 - IP, *see* IP, checksum
 - Kerberos message, 314
 - MAC, 345
- ches* (account), 129
- Cheswick
 - Kestrel, 2
 - Lorette Ellane Petersen Archer, xx, 2
 - Richard R., 2
 - Ruth, 2
 - Terry, 2
 - William, 287
- chfn* (program), 126
- children
 - are like employees, 241
- Chinese Lottery, **117**
- chmod*, 56
- chpass* (program), 126
- chroot, **162–167**
 - anonymous FTP and, 167
 - Apache Web server and, 165
 - application-level filters, 210
 - building a honeypot with, 295
 - CGI scripts, 167
 - chrootuid* and, 163
 - core dumps and, 162
 - denial-of-service from, 162
 - difficult to set up, 163
 - for CGI scripts, 165
 - IMAP and, 168
 - inetd* calls, 154
 - limitations, **162–163**
 - named* and, 170
 - POP3 and, 168
 - root* can break out of, 162
 - SMTP daemon and, 168
 - ssh* UsePrivilegeSeparation and, 158
 - suggested modification to, 166
 - support files in, 166
 - system call requires *root* privileges, 163
 - to a separate partition, 162
 - Web servers and, 66, 87
- chroot* (program), 163
- chsh* (program), 126
- chutzpah, 99
- CIDR (Classless Inter-Domain Routing), **21**
 - defines an intranet, 252
 - ipchains*, 219
- CIFS (Common Internet File System), 58
- CIO, 247
- Cipher Block Chaining, *see* CBC
- Cipher Feedback, *see* CFB
- Cipher Newsletter, 350
- ciphersuites, **83**
- ciphertext, **335**
- circuit gateways, *see* gateways, circuit level
- Cisco Netflow, 114
- Cisco routers
 - IP DEBUG, 114
 - patch information, 352
 - use configuration files, 214
- Citrix ICA
 - passwords sniffed by *dsniff*, 129
- CLARK (host), 310–312
- CLARK.RESEARCH.ATT.COM (host), 301
- Classless Inter-Domain Routing, *see* CIDR
- click-through license agreements, 275
- client programs, 23
- client pull, **274**
- client shim, **175**, 243
- clock, 64, 315
- clock skew limits, 317
- clog* (program), 275
- CNN, 290, 295

- Code Red worm, *see* worms, Code Red
- COM (host), 78
- COM.COM.COM (host), 78
- COM.EDU (host), 32
- COMDOTCOM.COM (host), 78
- Comer, Doug, 19
- command node, 110
- Commercial Off-The-Shelf, *see* COTS
- Common Gateway Interface, *see* CGI
- Common Internet File System, *see* CIFS
- common-mode failure, 67, 180
- Computer Emergency Response Team, *see* CERT
- Computers and Communication Security, *see* CCS
- conf (directory), 166
- configuration
 - disk space, 268
 - message-of-the-day, 268
 - routing, 268
- configure (program), 165
- connection filtering, **188**
- console
 - access, **271–272**
 - administration through, 267
 - local access only, 272
 - logins only allowed through, 264
 - RS-232 switch, 272
 - servers, 272
 - software switch, 272
- cookies, 75–76, 79
 - browsers configured to reject, 76
 - hackers put scripts in, 79
 - JavaScript can steal authentication data from, 82
 - recommendations about, 84
 - warnings in Netscape, 79
- COPS (program), 126, 268, 302
- copyright law, 56
- corporate, 9
- COTS (Commercial Off-The-Shelf), 153
- counter mode, **338**
- counterintelligence, 17
- CPU, 147
- crack, *see* hacking tools, crack
- CREEP, 105
- creeping featurism
 - in *inetd*, 267
- cribs, **336**
- cron (program), 60
- cross-site scripting slash, **82**
- cryptanalysis, 8, 15, 313
 - differential, 338
- cryptographic protocols, **335**
- cryptography, 11, 15–16, 63, 64, **313–328**, 335–347, *see also* encryption
 - asymmetric, *see* cryptography, public key
 - block cipher, 339
 - cipher block chaining mode, 339–340
 - cipher feedback mode, 341
 - client keys, 316
 - conventional, 337, 342
 - counter mode, 341
 - digital signature, *see* digital signatures
 - electronic code book mode, 339
 - encryption, *see* encryption
 - exponential key exchange, **343–344**
 - not authenticated, 344
 - initialization vector, 339–340
 - key, 335
 - key distribution systems, 343
 - legal restrictions, 314, 346
 - master keys, 314, 336, 342
 - modes of operation, 337, **339–341**
 - multi-session keys, 314
 - output feedback mode, 340
 - padding, 340
 - private key, 337–342
 - encrypted with passwords, 50
 - proprietary, 335
 - protocols, 313
 - timestamps in, 63
 - public key, 150, 326, **342–343**
 - disadvantages, 343
 - S-BGP, 30
 - secret key, *see* cryptography, private key
 - secure hash functions, 346–347
 - session keys, 314, 315, 317, 336, 342–344
 - symmetric, *see* cryptography, private key
 - timestamps, 347
 - on a document, 347
- cryptosystem
 - secret-key, 337

- cryptosystems, **313**
- csd*, 293
- cvs*
 - managing firewall rules with, 232
 - passwords sniffed by *dsniff*, 129
 - ssh* and, 238
- C preprocessor, 221

- D'Angelo, Diana, 287, 296
- D1 (host), 320
- D2 (host), 320
- daemon* (account), 166
- dangerous programs
 - wu-ftpd*, 167
- DARPA, **19**
- DASS, 328
- Data Encryption Standard, *see* DES
- database
 - authentication
 - troubles with, 144–145
- datagram, **20**, 27, *see also* UDP
- day-zero
 - backup, 270, **273**
- daytime* (program), 71
- DCE (Distributed Computing Environment), 48
- dd* (program), 273
- DDoS (Distributed Denial-of-Service), 107, **109–117**
 - attack tools, 131
 - trino*, 131
 - botnets and, 117
 - can only be mitigated, 107
 - diagram of, 110
 - flooding network links with, 108
 - hard to traceback, 107
 - mitigation, 111
- Debian Linux, 261
- DEC, 211, *see* Digital Equipment Corporation
- Decision, 290–295
- DECnet, xviii
- decryption, *see* cryptography
- DECstation 5000, 302
- defense in depth, **4**, 9, 15, 310
 - filtering e-mail, 206
- demilitarized zone, *see* DMZ
- demise, 15

- denial-of-service, *see* DOS
- DenyUsers, 156
- DES (Data Encryption Standard), 327, **337–338**
 - CBC mode, 326
 - modes of operation, 338
 - secure RPC uses, 48
 - used to secure SNMP, 326
- dessert topping, *see* floor wax
- destination unreachable, *see* ICMP, messages,
 - Destination Unreachable
- device driver, **19**
- dhclient* (program), 34
- DHCP (Dynamic Host Configuration Protocol), **33–34**, 38
 - comparison with DHCPv6, 36
 - firewall rules and, 219
 - relay, 34
 - war driving and, 242
- DHCPv6, **36**
- dial-up access, 256
- diceware, 142–143
- Dick Van Dyke Show, 291
- dictionary attacks, **96**
- Diffie-Hellman, 48, **343**
- dig*, 162
- dig* (program), 160, 162
- Digital Equipments, 78
- digital rights management, *see* DRM, 331
- Digital Signature Standard, *see* DSS
- digital signatures, **344–345**
 - of secure hashes, 346
 - of software packages, 270
- digital timestamp, **347**
 - link value, 347
 - linking, 347
- Dijkstra, Edsger W., 5
- DILBERT.COM (host), 90
- directed broadcast, 121
- directed broadcasts, **21**
 - disable forwarding of, 21
- directories
 - ... 127
 - X11 font library, 52
- dirty words, **186**, **204**
- discard* (program), 71
- discrete logarithm, **344**
- diskless workstations, 52

- Distance Vector Multicast Routing Protocol, *see* DVMRP
- Distributed Computing Environment, *see* DCE
- Distributed Denial-of-Service, *see* DDoS
- DMZ (demilitarized zone), **14–15**, 89, 160, 179
 - provisioning hosts on, 156
 - semi-secure software in, 255
 - used to interface between companies, 237, 249
 - Web servers should be in, 87
- DNS (Domain Name System), **31–33**, 72
 - alias for FTP server, 199
 - allowed between departments, 257
 - backup servers, 31
 - block zone transfers, 184
 - cache contamination, 32
 - commands
 - forwarder, 201
 - cross-checks, 32, 59, 201
 - dangerous misfeature, 32
 - dig* queries, 160
 - external service, 199
 - filtering, 198–201, 224
 - gateway's resolution, 201
 - internal access, 199
 - internal root, 199
 - internal service, 199
 - internal service of external names, 199–201
 - inverse queries, 32, 33
 - controlling, 32
 - lookup sequence, 32
 - permit UDP queries, 184
 - proposed KX record, 241
 - records
 - A, 31, 201
 - AAAA, 31
 - CNAME, 31
 - DNSKEY, 31
 - HINFO, 31, 32
 - MX, 31, 32
 - NAPTR, 31
 - NS, 31
 - PTR, 31, 32, 201
 - SIG, 31, 33, 34
 - SOA, 31, 160
 - SRV, 31
 - WKS, 31
 - rich source of target information, 32, 106
 - secondary servers, 33
 - sequence number vulnerability, 104
 - table of record types, 31
 - tree structure, **31**
 - tunnels and, 239
 - used to tunnel, 235
 - wildcard records, 32
 - zone example, 199
 - zone transfers, **31**, 33
- DNS proxy, 198
- DNSsec, **33**
 - needed for the KX record, 241
 - needed with VPNs, 239
 - predictions about, 330
 - spoofing tools widespread, 330
- domain and type enforcement, *see* DTE
- Domain Name System, *see* DNS
- dongle, *see* authenticator, handheld
- doorbell, 249
- Dorward, Sean, 310
- DOS (denial-of-service), 42, 71, 107–116, 159, 265, 266, 268
 - DHCP subject to, 34
 - exhausting disk space, 109
 - from *chroot* environments, 162
 - ICMP, 108, 209
 - IP source address spoofing, 107
 - remove *rpcbind* service, 48
 - syslogd* and, 159
 - Web servers and, 167
- downstream liability, **311**
- DRM (digital rights management), 275
- DS1, **185**
- dselect* (program), 270
- dsniff*, *see* hacking tools, *dsniff*
- dsniff* (program), 76, 123, 129
- DSO (dynamic shared object), 165
- DSS (Digital Signature Standard), 345
- DTE (domain and type enforcement), 163
- DUAL Gatekeeper, 215
- dump* (program), 273
- dumpster, 5
 - diving, **132**
- Dutch law, 297, 298
- DVMRP (Distance Vector Multicast Routing Protocol), 67

- Dynamic Host Configuration Protocol, *see* DHCP
- dynamic packet filter, *see* packet filters, dynamic
- dynamic shared object, *see* DSO

- E (host), 320
- e-mail, *see* mail
- eavesdropping, 8
 - on phone connections, 256
- eBay, 82, 332
- ECB (Electronic Code Book), 339
- echo* (program), 71, 72, 164
- eEye Digital Security, 119
- efficiency, 103
- eggs, 279
- egress filtering, **177**
 - asymmetric routes and, 115
- Eindhoven University, 297
- Einstein, Albert, 5
- Electronic Code Book, *see* ECB
- electronic emissions, 8
- electronic mail, *see* mail
- elvish, *see* fonts, Tengwar
- email, *see* e-mail
- EMBEZZLE.STANFORD.EDU (host), 288, 290
- Encapsulating Security Protocol, *see* ESP
- encapsulation, 67, **233**, 234
- encryption, 59, 234, 236, *see also* cryptography
 - AES, *see* AES
 - application level, 322–328
 - block cipher, 338
 - end-to-end, 242
 - preferred over link-layer encryption, 40
 - file, 8
 - first block, 339
 - key-id, 318
 - last block, 339
 - link level, **318**
 - mail, 326–327
 - network level, 318–322
 - SNMP, 326
 - stream cipher, 339
 - to authentication servers, 144
 - transport level, 319
 - triple, 342
- English Channel, 16
- ensniff.c* (program), 128
- entrapment, **17**
- environment variables
 - \$PATH, 52
 - TERM, 127
- erotica, 56
- error propagation, 340, 341
- es.c* (file), 305, 306
- ESMTP, 41
- ESP (Encapsulating Security Protocol), 318
- espionage, *see* industrial espionage
- ESPN.COM (host), 90
- Esser, Thomas, 435
- etc* (directory), 166
- etereal* (program), 160, 282
- Ethernet, 21–22
 - ARP and, 22
 - broadcasts ARP requests, 22
 - cut transmit wire to, 295
 - in hotels, 242
 - in the home, 239
 - monitoring packets on, 29, 182
 - monitoring with *tcpdump*, 295
 - private connections over, 262
 - rpcbind* designed for, 50
- ethics, 16–17
 - of counter infections, 56
 - scanning tools, 128–129
- ettercap* (program), 158
- exec* (program), 127
- expiration
 - key, 345
- expire* (program), 66
- exponential key exchange, 48, *see* cryptography,
 - exponential key exchange
- exponentiation, 343
- External Data Representation, *see* XDR
- extranets, **247**

- F (host), 320
- factoring, 343
- factors, **137**
- Family Educational Rights and Privacy Act, *see* FERPA
- FAQ (frequently asked questions), 128

- Farmer, Dan
 - in a hot tub, 241
 - on *finger*, 64
 - scanned Web server hosts, 129
- FEP (Firewall Enhancement Protocol), 228
- FERPA (Family Educational Rights and Privacy Act), 106
- FG.NET (host), 42
- field, **344**
- field* (account), 96
- file handle, *see* NFS, file handle
- file systems
 - Andrew, **52**
 - NFS, 51–52
 - prevent filling, 102
 - remote, 317
 - simulated, *see* jail partition
 - wiped out by hackers, 294
- File Transfer Protocol, *see* FTP
- files
 - hidden, 127
- filtering, 197–210, *see also* packet filtering
 - application level, 185–186, 226–227
 - circuit level, 186–188
 - DOS packets, 111–114
 - e-mail, 206–207
 - FTP, 202
 - GRE tunnels, 209
 - guidelines, 210
 - H.323, 208
 - ICMP messages, 209–210
 - IP over IP, 209
 - IPsec, 209
 - NTP, 203
 - POP and IMAP, 204
 - RealAudio, 208
 - SIP, 208
 - SMB, 209
 - SMTP, 203–204
 - ssh*, 206
 - TCP sessions, **202–203**
 - UDP, 207–208
 - Web, 202
 - X11, 209
- filtering bridge, **160**
- filtering languages
 - ipchains*, 216–220
 - ipfw*, 220
 - ipf*, 220–226
- find* (program), 308
- Finger
 - Diane, 2
- Finger* (program), 64
- finger*, **64**
 - gets hole in, 100
 - provides cracking information, 105
 - provides hacking information, 42
- finger* (program), 64, 65, 98, 100, 105, 293, 301
- fingerprint, 147
- fingerprinting, *see* hosts, fingerprinting
- Finisar, 160
- fink* (program), 270
- Firewalk* (program), 230
- firewalking, 121, **229–230**
 - avoided by IP-blocking gateways, 211
 - avoided with relays, 186
 - ipchains* allows, 217
 - with ICMP Path MTU messages, 209
- firewalking* (program), 229
- firewall
 - problems, **227–230**
- Firewall Enhancement Protocol, *see* FEP
- firewall rules, **212–214**
 - code walk-through, 232
 - inspecting, 232
 - samples, **216–226**
 - “temporary”, 228, 232
 - testing, 220
- firewalls, **11**, 13, **175–195**, *see also* gateways
 - administration, **230**
 - application-based, 226–227
 - as bulkheads, 253
 - building, **215–227**
 - bypassing with tunnels, 235
 - categories, 175
 - corporate, 257
 - departmental, 257–258
 - distributed, **193–194**
 - engineering, **211–232**
 - for an organization, **220–226**
 - FTP and, 229
 - history of, 211
 - implementation options, 188–190
 - ineffective on large perimeters, 253

- limitations of, 194–195
- placement, 257–258
- point, 258
- positioning, 253–255
- regression testing, 231
- replicated, 191–193
- rules and DHCP, 219
- rulesets, **212–214**
- simple, **216–220**
- testing, **230–232**
- using NAT, 38
- Web servers and, 89–90
- Firewalls mailing list, 199, 350
- first edition, xiii
- FLEEBLE.COM (host), 199
- floor wax, *see* dessert topping
- FMS attack, 39
- foistware, **69**, 241
- fonts
 - Hebrew *Hclassic*, 329
 - Tengwar, 95
- FOO.7ESS.MYMEGACORP.COM (host), 33
- FOO.COM (host), 32
- FOO.COM.BIG.EDU (host), 32
- FOO.COM.CS.BIG.EDU (host), 32
- FOO.COM.EDU (host), 32
- FOO.FLEEBLE.COM (host), 199
- forensics, 272, 303–311
 - DHCP logs, 34
 - needs accurate time stamps, 63
 - Radius logs, 34
 - using file access times, 308–309
- forgery, *see* spoofing
- forward, 200
- fragmentation, *see* packet filtering, fragmentation
- fragrouter* (program), 231, 280
- frame relay, 182
- France, 289
- FreeBSD, 165, 220, 261, 264, 270
 - field stripping, 266
 - ports collection, 270, 274
 - setuid programs on, 124
- frequently asked questions, *see* FAQ
- frobozz* (program), 210
- fsirand* (program), 51
- ftp* (account), 168
- ftp* (program), xiii, 4, 59, 138, 228
- FTP (File Transfer Protocol), **53–57**, 65, *see also*
 - ftpd*
 - anonymous, **55–57**, 65, 167–168
 - configuring, 168
 - attacks on, 60
 - bogus `passwd` file, 57, 98, 288, 290
 - bounce attacks, **55**
 - configuring, 57, 65, 109, 268
 - control channel, 53
 - data connection
 - over SSL on port 989, 171
 - denial-of-service with, 109
 - directory
 - publicly writable, 56
 - filtering, 202
 - firewalls and, 228
 - incoming, 57
 - over SSL on port 990, 171
 - passive, 103, 188
 - Web browsers, 77
 - passive data channel, **53–55**
 - passive is preferred, 55
 - passwords sniffed by *dsniff*, 129
 - processing in firewalls, 229
 - sample session, 54
 - spoken by Web browsers, 74
 - transfer modes, 55
 - tunneling with, 235
 - Web browsers and, 77
 - ftp PORT* (program), 228
 - ftpd*
 - commands
 - PASV, 53, 55, 188
 - PORT, 53, 188
 - TYPE I, 55
 - PASS, 103
 - USER, 103
 - configuring, 167–168
 - DNS cross-checking, 201
 - logging, 96
 - modifications, 167–168
 - privileges needed, 103
 - selecting version, 167
 - ftpd* (program), 167
 - FTPS, 171
 - FTPS-data, 171

- garlic
 - smb* likes, 287
- Gartner Group, 87
- gas mask, 290
- gateways
 - application level, 175, 199, 255
 - belt-and-suspenders, 255
 - circuit level, 175, 186–188, 199, 255, 280,
 - see also* tunneling
 - depends on correct router configuration, 9
 - fail-safe design, 9
 - has professional administration, 13
 - leaks, 236
 - mail, 186
 - packet filtering, 175
 - paranoid, 255
 - relay services, 187
 - FTP, 199
 - mail, 180, 199
 - netnews, 66
 - services, *see* services
 - simple administration, 12
 - topology, 180, 181
- gcc* (program), 261
- GECOS, 126
- Generic Security Service Application Program
 - Interface, *see* GSS-API
- gethostbyaddr, 32
- gets* (program), 155
- gets*, 100
- Ghengis Kahn, 5
- Glick, Paul, 287, 296
- Global Positioning System, *see* GPS
- glue routines, 47
- gnu keyring* (program), 142
- Goldberg, Ian, 38
- Google, 128, 351
- GPS (Global Positioning System), 63
- Grampp, Fred, 262
- graphical user interface, *see* GUI
- GRE tunnels, 30
 - filtering, 209
- Great Wall of China, 5
- grep* (program), 187, 219
- Groove Networks, 235
- Gross, Andrew, 123, 308
- group (file), 166
- GSS-API (Generic Security Service Application
 - Program Interface), 48, 327, 328
 - NFS servers, 51
- guest* (account), 12, 96, 295
- GUI (graphical user interface), 213
 - discussion, 213
 - in *ethereal*, 160
- Guninski, Georgi, 83
- GW (host), 179, 180, 200
- H.323, **46–47**
 - filtering, 188, 208
 - proxy, 215
- Haber, S, 347
- Hacker Off-the-Shelf, *see* HOTS
- hackers, **xix**
 - are out to get you*, 102
 - attacking Stanford, 289
 - attacks, *see* attacks
 - attacks stimulates tool production, 289
 - Dutch, 298
 - go after log files first, 159
 - goals, 8
 - legally untouchable, 299
 - malicious, 8, 159, 294
 - managing, 287
 - monitor Ethernets, 59
 - remove logs first, 60
 - tools, **119–133**
 - availability, 119
 - network monitoring, 295
 - wipe file systems, 294
 - would you hire, 132
- hackerz
 - doodz, 127
 - lamerz, 128
 - splotts, 122
 - warez, *see* warez
- hacking
 - attacks often launched on holidays, 308
 - goals, **121**, 301
 - recovery from, 127, **303**
- hacking tools, **128–131**
 - crack*, 129
 - dsniff*, **129–130**
 - nuke.c*, 27

- ethics, **128–129**
- hunt*, 118
- IP-Watcher*, 118
- Juggernaut*, 118
- juggernaut*, 130
- l0phtcrack*, 129
- nbaudit*, 58, 130
- nessus*, 131
- nmap*, 130
- Ping of Death*, 131
- trinoo*, 131
- Virus construction kits, 131
- handheld authenticator, *see* authenticator, handheld
- Hanlon's Razor, 227
- Hansen, Stephen, 289, 296
- hash2.0*, *see* *snefru*
- headhunters, 105
- helper applications, **79**
- hidden filenames, 127
 - with leading period, 123
- hijacking, *see also* TCP, hijacking
 - Web, 84
- Hoffman, J., *see* fonts, Hebrew *Hclassic*
- Hoffman, Joel, 435
- home directory, 60
 - FTP writable, 56
 - of system accounts, 60
- home networks, 239
 - employers often pay for, 239
 - home LAN security is hard, 241
 - linked to corporate intranets, 241–242
 - running SMB on, 169
- honeyd* (program), 130, 282
- Honeyman, Peter, 275
- honeypots, **281**
 - for Berferd, 295–298
 - misleading *nmap*, 130
 - with chroot, 295
- HOST A (host), 183
- host leaks, **236, 252**
 - detecting, 236
- HOST Z (host), 183
- host-based security, 253–255, 258
- HostbasedAuthentication, 154
- hosts
 - back doors into, **127**
 - breaking into, **122–126**
 - covering tracks, **126–127**
 - fingerprinting, 122, **130**
 - with ICMP Time Exceeded, 252
 - multi-homed, 23
 - obtaining *root* on, **123–127**
- hosts* (file), 199
- hosts.equiv* (file), 154
- Hotmail, 83, 203, 227
- HOTS (Hacker Off-the-Shelf), 22
- HP printer driver
 - scanned a network, 282
- HPUX
 - setuid programs on, 124
- HTML (Hypertext Markup Language), **74**
 - forms, 76
 - generated by JavaScript, 82
 - hidden fields in raw, 77
 - in attachments, 205
 - in e-mail to bypass JavaScript checks, 83
 - in HTTP responses, 75
 - inserted in user responses, 82
 - is easier than X11, 91
- HTTP (Hypertext Transfer Protocol), **65, 74–77**
 - authentication sniffed by *dsniff*, 76
 - cookies, *see* cookies
 - DELETE command, 76
 - GET command, 74, 76
 - LOCATION command, 75
 - maintaining connection state, 76–77
 - over SSL on port 443, 171
 - POST command, 76
 - PUT command, 76
 - query description, 74
 - REDIRECT command, 75
 - sample session, 74
 - server responses, 75
 - sessions, 76–77
- httpd* (program), 166
- httpd.conf* (file), 165, 166
- HTTPS, 171
- https
 - for administrative access, 184
 - implemented with *sslwrap*, 171
- Httpunnel* (program), 228
- Hushmail, 203
- Hussein, Saddam, 288

- Hypertext Markup Language, *see* HTML
- Hypertext Transfer Protocol, *see* HTTP

- i, 201
- IBM, 338
 - research, 168
 - Thinkpad, 332
- ICMP (Internet Control Message Protocol), **27–28**
 - can change routing, 27
 - denial-of-service with bogus packets, 108
 - Destination Unreachable, 28
 - DOS attacks, 108, 209
 - distinguishing “safe” and “unsafe” packets, 209
 - Echo Reply, 217
 - Echo Request
 - traceroute* and, 160
 - filtering, **209–210**
 - for v6, 28
 - Fragmentation Needed, 217
 - Need Fragment, 217
 - Path MTU Discovery, **27–28**
 - don’t block, 209
 - firewalking with, 209
 - Port Invalid
 - traceroute*, 209
 - Redirect
 - modify route tables with, 27
 - reports routing problems, 27
 - Time Exceeded, 217
 - traceroute* and, 160, 209
- ICMPv6, 28
- icons (directory), 166
- ICQ
 - connects to master servers, 46
 - passwords sniffed by *dsniff*, 129
- id_dsa.pub* (file), 156
- IDEA, 327
- ident* (program), 217
- identification, **137**
- Identification Friend or Foe, *see* IFF
- IDS (intrusion detection system), xv, 279
 - administering, 282
 - limitations of, **279–280**
 - placement of, 280–281
 - Shadow, 159
 - tools, **282–283**
 - types, 281–282
- IE, *see* MSIE
- IEEE 802.11, *see* 802.11
- IEFBR14.DLL* (program), 226
- IETF (Internet Engineering Task Force), 67
- IFF (Identification Friend or Foe), 145
- IGMP, **67**
- IKE (Internet Key Exchange), 318, 320
- IKEv2, 322
- IM (Instant Messaging), 45
- IMAP, **45**
 - filtering, 204
 - on medium-security hosts, 255
 - over SSL on port 993, 171
 - safe implementation of, 168–169
 - stack-smashing attack detected by *snort*, 283
- imap* (program), 149
- IMAPS, 171
- in.telnetd* (file), 306
- incoming
 - access policy, 184
 - access to port 2049, 52
 - calls, abuse, 187
 - FTP directory, 56
 - mail, 31, 177, 199
 - proxy use, 188
 - routing messages, 181
 - ssh, 199
- INDNS (host), 200
- industrial espionage, 32, 42
- inetd*
 - back door in, 127
 - discussion, 153–154
 - TCP wrappers and, 154
- inetd* (program), 43, 71, 87, 153, 154, 165, 169, 170, 267
- inetd.conf* (file), 267, 292
- information leakage, 105–106
- information security, 8
- information theory, **97**
- ingress filtering, **177**
- init* (program), 127, 216
- initialization vector, *see* IV
- input, 219

- INSIDE-NET (host), 185
- insiders
 - rejecting a firewall, 236
- installation, *see* configuration
- Instant Messaging, *see* IM
- instant messaging, 45–46
 - AOL, 45
 - ICQ, 46
 - IRC, 46
 - jabber*, 46
 - Microsoft Messenger, 46
 - SSL and, 46
- integrity checking, 15
- internal users, *see* insiders
- Internet
 - in the home, 331
 - mapping, 248
 - shutdown incoming access, 184
- Internet Control Message Protocol, *see* ICMP
- Internet Engineering Task Force, *see* IETF
- Internet Group Management Protocol, **67**
- Internet Key Exchange, *see* IKE
- Internet Liberation Front, 302
- Internet Printing Protocol, *see* IPP
- Internet Protocol, *see* IP
- Internet Relay Chat, *see* IRC
- Internet security
 - predictions about, 331–332
 - we are losing ground, 332
- Internet service provider, *see* ISP
- Internet Society, *see* ISOC
- Internet telephony, 46–47
- Internet Worm, 43, 100
- Interop, xiii
- intranet, 14, 60
- intranets, **247–258**
 - address allocation efficiency, 252
 - fax lines used to compromise, 248
 - host leaks, 252
 - leaks
 - routing, **248**
 - mapping, **248–249**
 - mergers and divestitures modify, 248
 - open routers on, 252
 - routing, **249**
 - statistics, 252
 - unknown connections into, 247
- intrusion detection, **279–282**
 - snort*, 282–283
 - port scans, 121
- intrusion detection system, *see* IDS
- IP (Internet Protocol), 19, **20–21**
 - broadcast, **67**, *see also* broadcast
 - checksum, 20
 - delivery isn't guaranteed, 20
 - filtering fragments, 228
 - fragmentation, 21
 - header, 19–21, 319
 - hops, 21
 - host address, 21
 - IP-transparent gateways
 - may force IP renumbering, 249
 - NAT and, 249
 - laundering
 - with circuit gateways, 187
 - multicast, 67
 - group, 67
 - network address, 21
 - options, 29, 179
 - filtering, 29
 - packets, 20
 - protocol 41 (6to4), 37
 - routing, *see* routing
 - source addresses are trustable, 20
 - source routing, 29, 179, 183, 255
 - loose, 29
 - spoofing, xiii, 20
 - backscatter from, 116
 - sequence numbers for, 72
 - tools available, 71
 - telephony, 46–47
 - TTL field
 - can limit Mbone distribution, 68
 - crude host fingerprinting with, 252
 - default values from SNMP queries, 62
 - finding distance to a firewall with, 230
 - gives clues to attacker's distance, 114
 - low values in a DOS attack, 113
 - small values can fool an IDS, 280
 - traceroute* uses, 160
 - tunneling, 234, 319
 - with DNS, 235
 - tunneling IPv6 packets, 36–37
 - unicast, 67

- use of bogus addresses internally, 183
- IP addresses
 - allocating, 249
 - intentional misuse of, 249
- IP over IP, **235**
 - filtering, 209
- IP Security Policy, *see* IPSP
- Ipchains, 220
- Ipchains* (program), 216, 220
- ipchains*, *see* filtering languages, *ipchains*
- ipchains* (program), 214–216, 219, 220
- ipchains -L* (program), 218
- ipchains-restore* (program), 218
- ipchains-save* (program), 218
- ipchains-save input* (program), 218
- Ipf* (program), 226
- ipf*, *see* filtering languages, *ipf*
 - can filter tunneled IPv6 traffic, 37
- ipf* (program), 37, 214, 215, 220, 221
- ipf.conf* (file), 221
- ipf.conf.restrictive* (file), 221
- ipftest*, **226**
- ipftest* (program), 226
- ipf*, *see* filtering languages, *ipfw*
- ipfw* (program), 214, 216, 220
- iplog* (program), 130
- IPP (Internet Printing Protocol), 235, 264
- IPsec, 118, 242, 271, **318–322**
 - AH, **318–319**
 - broken by Windows reconfiguration, 243
 - configuring is hard, 243
 - ESP, **318–319**
 - filtering, 209
 - graph of possible configurations, 321
 - interactions with NAT, 242
 - key management, **320–322**
 - keys compromised by malware, 243
 - NAT and, 38
 - placement, 319–320
 - Windows applications and, 243
- IPSP (IP Security Policy), 320
- Iptables* (program), 216
- IPv4, *see also* IP
 - address format, 21
 - multicast, 67
- IPv6, **34–37**, 126
 - address formats, 35–36
 - anycast addresses, 35
 - DHCPv6, **36**
 - economic drivers?, 330
 - Filtering, 36–37
 - hardware acceleration in routers, 329
 - link-local addresses, 36
 - multicast, 36
 - ND, **36**
 - network numbers may change frequently, 35
 - predictions about, 329–330
 - site-local addresses, 35
 - supported on UNIX-like platforms, 329
 - tunneling through IPv4, 36–37
- Iraq, 288
- irc* (program), 219
- IRC (Internet Relay Chat), 117, **349**
 - passwords sniffed by *dsniff*, 129
 - used to control botnets, 117
- IRC* (program), 46
- Irix 6.2, 166
- ISDN, 46
- ISOC (Internet Society), 353
- ISP (Internet service provider), 58, 114
- ISS, 131
- IV (initialization vector), 39, 326, 339, 340
- jabber* (program), 46
- jail, *see* chroot
- jail* (program), 163, 165, 167
- jail partition, 295–299
- Java, **80–82**, 264, 277
 - native methods, 81–82
 - resistant to buffer overflows, 210
 - Web browser controls for, 84
- Java Web Server, **82**
- JavaScript, **82–83**, 264, 277
 - bypassing deactivation of, 83
 - cross-site scripting, 82
 - Web browser controls for, 84
- Jeeves, **82**
- Jerusalem, 290
- juggernaut*, *see* hacking tools, *juggernaut*
- k5su* (program), 126

- KDC (Key Distribution Center), 150, 314, 336
 - external, 316
 - must be available in real time, 342
 - safeguarding, 15
- keep it simple, stupid, *see* KISS
- Kerberized Internet Negotiation of Keys, *see* KINK
- Kerberos, 11, 150, **314–317**, 328
 - attacks on initial ticket, 317
 - authentication, 313
 - authenticators, 317
 - connecting outside realm, 316
 - in *ssh*, 157
 - in Windows 2000, 313
 - instance, 314
 - key distribution, 314
 - limitations of, 316–317
 - no handheld authenticators for, 317
 - primary name, 314
 - principal, 314, 315
 - realm, 314
 - ticket, 314
 - ticket-granting ticket, 317
 - variant of X11, 71
- Kerberos V4
 - bugs in, 262
- kernel
 - configuration, *see* configuration, kernel
- key
 - cache, 316
 - database, 50, 146, 147
 - distribution, 15, 314, 320, 327
 - Kerberos, 314
 - distribution problems, 71
 - escrow, 15
 - expiration, 345
 - exponential exchange, 48
 - lifetime, 318
 - session, 48
 - stealing, 336
- Key Distribution Center, *see* KDC
- keyinfo* (program), 126
- keyinit* (program), 126
- keyrings, **327**
- killer packets, **108**
- KINK (Kerberized Internet Negotiation of Keys), 320
- KISS (keep it simple, stupid), 212
- known-hosts* (file), 323
- Koblas
 - David, 187
 - Michelle, 187
- Kolstad, Rob, 108
- L0pht
 - AntiSniff, 159
 - L0phtcrack*, 129
- L2TP (Layer Two Tunneling Protocol), 235
- Lamport, Leslie, 146
- LAN
 - misconfigured router on the gateway, 182
 - network encryption on, 320
- LanManager, *see* Windows NT, LanManager
- laptop, 156
- Large Installation Systems Administration, *see* LISA
- lastlog* (file), 127
- L^AT_EX, 270, 435
- Laugh-in, 42
- laundering connections, *see* attacks, connection
 - laundering
- law enforcement, xix
 - notifying when attacked, 311
- Layer Two Tunneling Protocol, *see* L2TP
- lib.aa* (file), 309
- ldap* (program), 149
- LDAP (Lightweight Directory Access Protocol), **65**
 - PGP keys distributed with, 327
- leaks
 - host, 236, 252
 - routing, 182, 236, 251
- least privilege, **5**, **102**, 212
- Leech, Marcus, 117
- lex* (program), 102
- lib.msg* (file), 309
- lib/codepages* (directory), 169
- lib/etc/smbpasswd* (file), 169
- libpcap* (program), 282
- library, *see also* shared libraries
 - get host names, 32
 - X11 font, 52
- libtool* (program), 165

- Lightweight Directory Access Protocol, *see* LDAP
- Limoncelli, Tom, xvi, 87
- link level
 - encryption, **318**
- link-local address, 36
- Linux, xviii, 163, 220, 264, 270
 - Debian, 261
 - field stripping, 266
 - for a cheap firewall box, 257
 - in hardware VPN product, 244
 - increasing target for viruses, 106
 - often defaults to all services turned off, 255
 - personal firewall for, 215, **216–220**
 - Red Hat, 261
 - have public key in ROM BIOS?, 332
 - RPMS and, 270
 - secure, 163
 - setuid programs on, 124
 - Slackware, 261
 - Slapper worm and, 111
 - ipchains*, 214
 - supports IPv6, 329
 - uses client pull, 274
- lip-print, 147
- LISA (Large Installation Systems Administration), 353
- load average, 43
- lock* (program), 126
- lockpicking, 120
- locks
 - automobile, 6
 - hotel doors, 6
- locks (directory), 169
- log (directory), 166
- logged-in, 219
- logged-out, 219
- logging, 8, 158–159, **272–273**
 - drop safe, 159, 272
 - needs disk space, 268
 - off-machine, 159
 - synchronized with timestamps, 63
 - TCP destination, 187
 - with *rpcinfo* command, 48
- login* (program), xvii, 58, 95, 96, 127, 164, 295, 297
- logs, *see also* logging
 - altering, 126
 - logs (directory), 166
 - Los Alamos, 289
 - loss of life, 16
 - Love bug worm, 243
 - lpq* (program), 126
 - lpr* (program), 126
 - lprm* (program), 126
 - ls* (program), 52, 57, 99, 123, 304, 305
 - Lumeta Corp., 248, 252
 - lures, *see* honeypots
- m4, 221
- MAC (message authentication code), 315, 340, 347
- Mac OS/X
 - uses client pull, 274
- Macintosh
 - Rendezvous* service, **264**
 - configuration, 264
 - OS/X.2, 264
 - virus target, 106
- magic cookie, **71**
- mail, 41–45, 179
 - aliases on gateway, 42
 - aliases provide hacking clues, 42
 - application gateway, 186
 - bombing, 108
 - cryptographic, 100
 - delivery, 180
 - delivery through a packet filter, 178
 - expertise at gateway, 42
 - filtering policy discussion, 203–204
 - gateway, 186
 - headers, 42
 - incoming, 177
 - mailing list, 42
 - multimedia, *see* MIME
 - return address not reliable, 42
- mail* (program), 201
- MAILGATE (host), 185
- mailing list
 - firewalls*, 350
 - bugtraq*, 350
 - vuln-dev, 350
 - VulnDiscuss, 350

- VulnWatch, 350
- man, 129
- managed code, **263**
- management information base, *see* MIB
- manzier, 282
- mapping
 - intranets, 248–249
 - the Internet, 248
- Markoff, John, 298
- masquerading, **216**
- MBone, **67–68**
 - ports, 67
- MD5, 327, 347
- mDNS protocol, 264
- media, xix
- Meeting Maker
 - passwords sniffed by *dsniff*, 129
- Melissa worm, 106, 205, 243, 253
- message authentication code, *see* MAC
- MIB (management information base), 62
- micro_httpd* (program), 87
- Microsoft
 - .NET, **263–264**
 - risks, 264
 - ActiveX, **80**, *see* ActiveX
 - CIFS proposed by, 58
 - DOS commands, 123
 - IIS, 87
 - Internet Explorer, *see* MSIE
 - Messenger, 46
 - NetMeeting, 46
 - Office, 205
 - Outlook Express, 44
 - PPTP authentication, 129
 - reserves right to change software on a host, 275
 - RPC and, 47
 - security initiative, 330–331
 - signs ActiveX with digital signatures, 270
 - SMB protocol used by, 57
 - SMS, 193
 - source code unavailable, 114
 - SQL passwords sniffed by *dsniff*, 129
 - uses client pull, 274
 - will support IPv6, 329
 - Windows, *see* Windows
 - Windows Media Player, 274
 - Word, 205
 - examining files in UNIX, 205
 - Word macros, 131
 - Wordpad, 213
- Microsoft Internet Explorer, *see* MSIE
- Middle East, 293
- military, 9
- milk, adulterated, 120
- MIME (Multipurpose Internet Mail Extensions), **43–44**, 65
 - uses PostScript, 44
- `mime.types` (file), 166
- mind, boggled, 16
- minimal trust, **43**
- MIT, 113, 314
- MLS (multilevel secure system), 10
- moat, 204
- mobile hosts, 234
- modes of operation, *see* cryptographic, modes of operation
- Mogul, Jeff, xx, 229
- monitoring, 58–60, 290, 295–296, 326
 - tools, 289
 - wiretap, 8, 96
- monoculture, 89, 106, **112**
- monsters
 - cookie, 75
 - moat, 204
- Morris Worm, *see* worms, Morris
- Morris, Bob, 59, 98, 100
- Morris, Robert (*not* junior), 23–24
- mrinfo* (program), 126
- MS-DOS, xviii
- MSIE (Microsoft Internet Explorer), *see also*
 - Web browsers, 83
 - ActiveX and, 80
 - defaults to FTP PORT command, 55
 - S/MIME in, 326
- mtrace* (program), 126
- MTU discovery
 - permitted in filter, 217
- Muffett, Alec, 129
- multi-homed host, 23
- multicast, 68, *see* IP, multicast
 - backbone, *see* MBone
 - routers, 67
 - session directory, 67

- multilevel secure system, *see* MLS
- Multipurpose Internet Mail Extensions, *see* MIME
- Muus, Mike, 131
- MYBANK.COM (host), 78

- NAI Sniffer
 - passwords sniffed by *dsniff*, 129
- naim* (program), 46
- name service, *see also* DNS
 - attacks on, 149
 - dumping the database, 162
 - external, 201
 - internal, 201
- named
 - safe implementation of, 170
- named* (program), 170
- NANOG (The North American Network Operators' Group), 110
- Napster
 - passwords sniffed by *dsniff*, 129
- NAS (Network Access Server), 148
- NASA, 67
- Nass, Simona, 242
- nat* (program), 130
- NAT (Network Address Translation), 37–38
 - as a firewall, 38
 - in hotel networks, 242
 - incompatible with some kinds of encryption, 38
 - interactions with IPsec, 242
 - private address space and, 37
- National Bureau of Standards, 338
- National Security Agency, *see* NSA, 338
- native methods, **81**
- nbaudit*, *see* hacking tools, *nbaudit*
- nbaudit* (program), 58
- NBC Dateline, 309
- NBS, *see* National Bureau of Standards
- NCR
 - setuid programs on, 124
- ND (Neighbor Discovery), 36
- NDSS (Networks and Distributed Systems Security), 353
- Neighbor Discovery, *see* ND
- Neighbor Solicitation, **36**
- nessus*, *see* hacking tools, *nessus*
- nessus* (program), 351
- NET (host), 78
- NET 1 (host), 180, 182, 183
- NET 100 (host), 183
- NET 2 (host), 179, 180, 182
- NET 3 (host), 179, 180, 182
- NetBIOS, 169
 - block with departmental firewalls, 257
- netbios* (program), 214
- NetBSD, 164, 261, 270
 - field stripping, 266
 - setuid programs on, 124
- Netherlands, 297
- NetInfo* (program), 264
- NetMeeting, 237
 - uses UDP packets, 215
- netnews, 66
 - on a gateway, 66
 - processing on the gateway, 66
 - resource hog, 66
 - security holes in, 66
- NetOptics, 160
- Netscape, *see also* Web browsers
 - can display cookie warnings, 79
 - S/MIME in, 326
 - uses client pull, 274
- netstat* (program), 267, 295, 303
- netstat -a* (program), 226
- netware, xviii
- network
 - backup links, 183
 - elements, **265**
 - configuring with GUIs, 213
 - control with SNMP, 326
 - default passwords not changed in, 265
 - frequent reconfiguration of, 265
 - monitoring, 271
 - ROM updates, 274
 - SNMP management of, 62
 - Web configuration of, 91
 - layers
 - diagram of, 20
 - scanners, **121–122**
 - locating hosts with, 121
 - scanning
 - by HP printer driver, 282

- standard management tools, 236
- topology, 183
- Network Access Server, *see* NAS
- Network Address Translation, *see* NAT
- Network File System, *see* NFS
- Network Flight Recorder, *see* NFR
- Network IDS, *see* NIDS
- Network Information Service, *see* NIS
- Network News Transfer Protocol, *see* NNTP
- Network Time Protocol, *see* NTP
- Networks and Distributed Systems Security, *see* NDSS
- New York Times*, 43, 298, 347
- Newsday, 309
- newsgroups
 - comp.risks*, 350
 - proprietary, 66
- NFR (Network Flight Recorder), 214
- NFS (Network File System), **51–52**, 264
 - blocked from outside at a university, 184
 - disable setuid programs over, 52
 - file handle, **51**
 - stale, 51
 - is (mostly) stateless, 51
 - passwords sniffed by *dsniff*, 129
 - port numbers, 51–52
 - root* access prohibited, 51
 - root* file handle, 51
 - ssh* and, 105
 - suspicious access to, 208
 - Version 3, 52
- nice* (program), 162
- NIDS (Network IDS), 279
- Nimda worm, 83, 87
- NIS (Network Information Service), **50**, 98
- NIST, *see* National Bureau of Standards, 345, 347
- nmap*, **130**
- nmap* (program), 130, 131, 226, 282
- nmapNT* (program), 119
- nntp* (program), 66
- NNTP (Network News Transfer Protocol), **66–67**
 - spoken by Web browsers, 74
- nntpd* (program), 66, 67
- nobody* (account), 169
- nohup* (program), 309
- nohup.out* (file), 309
- Northcutt, Stephen, 159
- NOYFB, 84
- NSA (National Security Agency), 5, 100, 338
- NSF
 - block with departmental firewalls, 257
- nslookup* (program), 160
- NTBugtraq, **350**
- ntp* (program), 63, 126
- NTP (Network Time Protocol), **63–64**
 - filtering, 203, 225
 - on medium-security hosts, 255
 - permit access, 184
 - relatively safe UDP protocol, 208
- NTP.INSIDE (host), 184, 185
- NTP.OUTSIDE (host), 184, 185
- ntpdate* (program), 126
- nuke.c* (program), 128
- od* (program), 305
- OFB (output feedback), 340, 341
- one-factor authentication
 - in *ssh*, 154–156
- One-Time Password, *see* OTP
- one-time passwords, *see* passwords, one-time
- onion, *see also* garlic
 - ches* doesn't like, 287
- open* (program), 127
- open relays, **43**, 204
- Open Shortest Path First, *see* OSPF
- open source, 261
 - discussion of, 270
- OpenBSD, 261, 270
 - field stripping, 266
- OpenPGP, **327**
- OpenSSH* (program), 61, 154, 270, 275
- OpenSSL* (program), 89
- Oracle
 - SQL*Net, **68–69**
 - passwords sniffed by *dsniff*, 129
- oracles, **337**
- Orange Book, **11**, 102, 261
 - access controls, 11
 - and the Morris Worm, 102
 - auditing, 11
- ORG (host), 78

- OS/X, 270
 - field stripping, 266
- OS/X.2, 220
- OSF, 48
- OSPF (Open Shortest Path First), 29
 - authentication, 29
 - passwords sniffed by *dsniff*, 129
- OS X, 220
- OTP (One-Time Password), 98, 104, 146
- Oulu University, 62
- OUR-DNS (host), 184
- OUR-GW (host), 177
- OURHOST (host), 178
- outgoing
 - access policy, 184
 - laundering calls, 8
 - mail headers, 42
 - packet filtering, 178
 - restrictions, 7, 8
 - UDP packets, 208
- output feedback, *see* OFB
- outside world, xviii

- p2p, **69**
- packet filtering, 175, **176–185**, 207
 - block UDP port 2049, 52
 - bridge, 160, 161
 - by subnet, 178
 - CERT recommendations, 350
 - departmental firewalls, 257
 - DNS, 184, 185, 198–201
 - dynamic, **175, 188–193**
 - asymmetric routes and, 191
 - safety of, 193
 - erroneous, 178
 - fragmentation, 228–229
 - high port numbers, 67
 - ICMP, 209
 - IP fragmentation, 228
 - MBone can subvert, 67
 - outbound calls, 178
 - performance, 185
 - reject packets with options, 29
 - removed or erroneous, 9
 - requires expertise, 177
 - routing, 182–183, 235
 - RPC, 188
 - rpcbind*, 50
 - sample configurations, 184
 - TCP considerations, 178
 - UDP, 207–208
 - UDP is very hard, 207
 - XDR is hard, 48
- packet storms, 72
- packet telescope, **116**
- pages (directory), 166
- Palm Pilot, 142
- palm tops
 - storing passwords on, 142
 - viruses in, 131
- PAM (Pluggable Authentication Module), 158
 - ssh* and, 158
- Panix, 109, 111, 112
- paranoia, 9, 180
- Parseghian, Pat, 302
- Passface, 142
- passwd* (file), 56
- passwd* (program), 293
- password safe* (program), 142
- passwords, 95–98, 138–147
 - aging is bad, **138–140**
 - converted to Kerberos key, 315
 - cracking, 98, 288, 317
 - diceware, **142–143**
 - files
 - Berferd wanted to modify, 290
 - bogus, 57, 288
 - distributed by NIS, 50
 - in FTP directory, 56
 - shadow, 98
 - simulated for Berferd, 294
 - stealing, 98
 - gateway administrative, 160
 - given out by NIS, 50
 - guessing, 53, 64, 96
 - by Berferd, 287
 - with *finger* information, 105
 - hidden costs of, 143
 - human choose lousy, 96
 - in exponential key exchange, 344
 - in router configuration files, 53
 - keyrings, **142**
 - keys generated from, 15

- Lamport's algorithm, **146–147**
- list needed by the authors, 141
- machine-chosen, 139
- not reliable on tapped lines, 59
- null *root*, 272
- on different hosts, 99
- one-time, 59, **144–147**, 302, 310, 342
 - challenge/response, 145–147
 - don't stop TCP hijacking, 59
 - Plan 9 uses, 310
 - paces, 104
 - remote console access with, 272
- optimum length, 97
- poorly chosen, 14
- protecting, 98
- shadow, 50, 98
- sniffing, 96, 310
- stealing, 29, **58–59**, 96, 99, 128, 160
 - big-time, 187
 - by monitoring, 103
- time-based, **144–145**
- user-chosen, 138
- Path MTU discovery, *see* ICMP, messages,
 - path MTU discovery
- PAYPAI.COM (host), 325
- PC, 59, 103, 146, 184
- PC card
 - smart cards, 147
 - VPN boxes, 243
- PCLAB-NET (host), 184
- peer-to-peer
 - file transfers, 192
 - networking, **69–70**
 - large networks not suitable for Kerberos, 317
 - possible IPv6 application, 330
 - security doesn't scale well, 69
 - NTP, 208
 - SIP phones, 47
 - SOAP, 235
 - with firewalls, 46
 - worm network, 111
- Pentium, 266
- perimeter
 - security, **10–11**
 - too large, 11
- Perl
 - script
 - generated by *htp*d, 66
 - implements a Web server, 45
 - scripts
 - CGI scripts, 166
 - used for CGI scripts, 86
- perl* (program), 219
- personal identification number, *see* PIN
- pessimism, 11
- PGP (Pretty Good Privacy), 326
 - and transmission security, 327
 - attachments, 205
 - cryptology, **327**
 - file encryption, 57
 - keyrings
 - cracking, 129
 - keys encrypted with a passphrase, 139, 142
 - public key for contacting hackers, 302
- philosophy, 178
 - authentication, 99–100
 - clients vs. servers, 85
 - defense in depth, 310
 - least privilege, **5**, 102, 262
 - repeated warnings, 79
 - user security specifications, 83
- phone book
 - determine organizational structure with, 105
 - network service, xvii
 - online, 105
- phone connections
 - eavesdropping on, 256
- PHP (PHP Hypertext Preprocessor), **86**
- PHP Hypertext Preprocessor, *see* PHP
- Phrack*, 130, 349
- physical access, 260
 - alternatives to, 271
 - host administrators should use, 260
 - reading password posted on a terminal, 99
 - to console, 122
- physical perimeter, xvii
- PIN (personal identification number), 146, 147, 342
- ping, *see* ICMP, messages, Echo Request
- ping*, 160
- ping* (program), 27, 113, 160, 183, 209, 215, 240, 248

- Ping of Death*, *see* hacking tools, *Ping of Death*
- ping6* (program), 126
- pirated software, 56
- Piscitello, David M., 28
- PKI (Public Key Infrastructure), 30, **150–151**
- PKIX (Public Key Infrastructure (X.509)), 322
- plaintext, **335**
- Plan 9, 310
 - authentication, 310
- playback monitored terminal sessions, 296
- PLAYCRITTER.COM (host), 90
- Pluggable Authentication Module, *see* PAM
- point firewalls, 258
- Point-to-Point Protocol, *see* PPP
- Point-to-Point Tunneling Protocol, *see* PPTP
- police, xix
- policy
 - default, 10
 - disconnection, 9
 - firewall, 54
 - importing foreign software, 7
 - made by users, 60
 - outgoing traffic, 7
 - personal use, 7
- POP3, **44–45**
 - APOP authentication, 45, 145, 204
 - filtering, 204
 - on medium-security hosts, 255
 - over SSL on port 995, 171
 - safe implementation of, 168–169
 - SSL and, 45
- pop3* (program), 145, 149
- POP3S, 171
- PORT* (program), 228
- PORT, 202
- port scan
 - for RPC services, 50
- port scanners, 121–122
 - SYN only, 122
- portmapper* (program), 48, 49
- postern gate, *see* back doors
- postfix*, **168**
- postfix* (program), 126, 168
- PostgreSQL
 - passwords sniffed by *dsniff*, 129
- postmaster
 - knows SMTP commands, 42
 - located with SMTP `VERFY` command, 42
- PostScript
 - called by MIME, 44
 - can be dangerous, 44
- ppp* (program), 126, 145
- PPP (Point-to-Point Protocol), 235
- PPTP (Point-to-Point Tunneling Protocol), 235, 242
 - encrypted, 271
 - MS-CHAP
 - passwords sniffed by *dsniff*, 129
- pre-IV, 326
- predictions, 329–332
 - DNSsec, 330
 - from the first edition, xiv
- Presotto, Dave, 187, 262
- Pretty Good Privacy, *see* PGP
- prime numbers, 343
- privacy, 16, 326
- private address space, **37**
 - choosing, 183
- privileged ports, 48
- programming advice, 102–103
- Project Athena, 314
- promiscuous mode, 182
- propeller-heads, 122
- protocol
 - encapsulation, 234
 - failures, 104–105
 - layers, 19
 - proprietary, 68–69
- protocols
 - mDNS, 264
 - NetInfo, 264
- Provos, Niels, 275, 282
- proxies, **214–215**
 - DNS, 198, 207
 - for ActiveX, 202
 - FTP, 189, 202
 - H.323, 208, 215
 - scan for malware, 202
 - transparent, 215
 - Web, 202
- ps*
 - ignores hacker's program, 127
- ps* (program), 127, 267, 292, 295, 297, 303

- PSTN (Public Switched Telephone Network), 271
- public key, *see* cryptography, public key
- Public Key Infrastructure, *see* PKI
- Public Key Infrastructure (X.509), *see* PKIX
- Public Switched Telephone Network, *see* PSTN
- Puddin'head Wilson, 279
- Punoval, Theophilus, 159
- putty* (program), 61
- puzzle palace, *see* National Security Agency
- pwd.db* (file), 166
- Python, Monty, 239

- Q.931, 46
- quota* (program), 126

- r*-commands, **59–61**
 - authentication rules, 59
- RA (Router Advertisement), 36
- races
 - booting a firewall, 220
- RADIUS (Remote Authentication Dial In User Service), 34, 148
- radiusniff* (program), 123
- Rainbow Series, **101**
- random numbers
 - generating, 340
 - in attack packets, 111
 - NFS file handles, 51
- Ranum, Marcus, 166, 167, 228
 - Ranum's Law, 202, 204
- rcp* (program), 61, 126, 322
- rdist* (program), 61, 154, 274
- RDX, *see* cclotrimethylenetrinitramine207
- read* (program), 88
- Real Networks, 68
- Real-Time Transport Protocol, *see* RTP
- RealAudio, 68
 - filtering, 208
- RealPlayer* (program), 274
- Received:, 33
- recursion, *see* recursion
- Red Hat Linux, 261
- Red Hat Package Manager, *see* RPM
- Reed, Darren, 220

- regression testing, 231
- relay, *see* gateways, relay services
- Remote Authentication Dial In User Service, *see* RADIUS
- Remote Procedure Call, *see* RPC
- Rendezvous* (program), 264
- replay attacks, *see* attacks, replay
- replicated firewalls, 191–193
- resolv.conf* (file), 200
- resource record, *see* RR
- retarget* (program), 169
- rexeed* (program), 96
- RFC 822, 185, 289, 291
- RFC 1122, 29
- RFC 1123, 24
- RFC 1149, 235
- RFC 1918, 176, 183, 242, 249
 - typical address usage on corporate networks, 254
- RFC 1948, 25
- RFC 2549, 235
- RFC 2822, 43
- RFC 3056, 37
- RFC 3195, 159
- RhostsRSAAuthentication, 154
- RIP (Routing Information Protocol), 29
 - passwords sniffed by *dsniff*, 129
- Risks Forum, **350**
- Ritchie, Dennis, 266
- Rivest, Ron, 339, 343
- Riyadh, 292
- rkdet* (program), 125
- rld* (program), 163
- rlogin* (program), xiii, 11, 13, 32, 59–61, 89, 126, 127, 138, 154, 168, 183, 292, 322, 387
- rlogin.myhost* (account), 314
- rlogind* (program), 29, 61
- rm* (program), 16, 126, 294
- rm -rf/*, 294
- roach motel, *see* jail partition
- Roesch, Martin, 282
- root* (account), 11, 23, 43, 45, 50, 51, 55, 56, 60, 61, 66, 71, 103, 121, 123–128, 138, 153–155, 158, 162–165, 168–170, 210, 264, 269, 272, 275, 288, 290, 294, 298, 303, 304, 306, 311, 314

- root* access
 - easy to get in UNIX, 311
- root partition, 273
- rooted domain name, **32**
- rootkit, **125–126**, 128
- route* (program), 126
- route squatting, **183**
- routed* (program), 268
- ROUTER (host), 181
- Router Advertisement, *see* RA
- routers, **21**
 - access to network provider's, 181
 - booted with TFTP, 52
 - configuration files, 53
 - deflecting routing attacks, 29
 - multicasting, 67
 - network provider's, 53
 - packet filtering, 177
 - performance, 185
 - predictions about security, 331
 - replaced every 18 months, 329
 - swamped by UDP packets, 27
- routing, 28–29
 - asymmetric, **28**, 160
 - can't eliminate, 192
 - dynamic packet filters and, 191
 - egress filtering and, 115
 - with dynamic packet filters, 191
 - attacks, *see* attacks, routing
 - between companies through a home network, 241
 - CIDR, 21
 - default route, 182
 - filtering, *see* packet filtering, routing
 - ICMP can change, 27
 - IPv6 prefix announcements, 36
 - leaks, 182, 236, 248, **251**
 - loose source, **29**
 - on intranets, **249**
 - protocol
 - IS-IS, 29
 - protocols, 29
 - static, 268
 - subversion by route confusion, 183
 - trouble reporting with ICMP, 27
- Routing Information Protocol, *see* RIP
- RPC (Remote Procedure Call), **47–52**
 - authentication, 48
 - Microsoft uses, 47
 - procedure number, **48**
 - program number, **48**
 - secure, **48**
 - DCE use of, 48
 - sequence number, **48**
 - sequence number vulnerability, 104
 - stub routines, **47**
 - uses random port numbers, 208
- rpcbind, **47–50**
- rpcbind*
 - forwards screened requests, 103
 - indirect calls, **50**
 - table of sample services, 49
- rpcbind* (program), 48–50, 52, 69, 267
- rpcinfo* (program), 48
- RPM (Red Hat Package Manager), 270
- RR (resource record), 31
- RS-232
 - console switch, 272
- RSA, 327, **342–343**
- RSA Security, 326
- RSADSI, 339
- rsh* (program), 56, 59–61, 98, 103, 126, 154, 322, 387
- rshd* (program), 29
- rstatd* (program), 123, 267
- rsync* (program), 57, 154, 156, 193, 274
- RTP (Real-Time Transport Protocol), 47
- Rubin
 - Ann, 2
 - Benny, 2
 - Elana, 2
 - Mendl, 2
 - Tamara, 2
- RUBINLAP (host), 217
- rulesets, **212–214**
- S-BGP, 30
- S-box (substitution box), 338
- s.c* (program), 307
- S/Key, **146**
- S/MIME, 326
 - encryption, **326–327**
 - transmission security, 327

- SA (security association), 322
- SAC (Strategic Air Command), 231
- safe haven, **259**
- SALES.MYMEGACORP.COM (host), 42
- Samba
 - on medium-security hosts, 255
 - safe implementation of, 169–170
- samba* (program), 58, 169
- sandbox, **82**, **162**, *see also* chroot
 - chroot*, 162
 - Java, 162
- SASL (Simple Authentication and Security Layer), 149
- SATAN, 131
- satellite links, 318
- sbox* (program), 86
- Schneier, Bruce, 351
- Scotland Yard, 16
- scp* (program), 61, 154, 156, 273
- screend* (program), 229
- script kiddies, **123**
- SCTP (Stream Control Transmission Protocol), **25–27**
 - and SIP, 47
- Scuds, 290, 291
- SECONDARY (host), 184, 185
- secure hash functions, 146, *see* cryptography,
 - secure hash functions
- secure hosts, **259–277**
 - access to, 271–272
 - administering, 271–277
 - definition of, 259
 - field stripping a UNIX host, 266–270
 - hardware configuration, 265–266
 - properties of, **260–265**
 - software guidelines for, 260–262
 - updating software, 274–275
 - Web servers, **86–87**
- Secure Multipurpose Internet Mail Extensions,
 - see* S/MIME
- Secure RPC, *see* RPC, secure
 - key database, 50
- Secure Socket Layer, *see* SSL
- secure software
 - properties of, 260–262
- SecurID, 144
- security
 - “minimal trust” philosophy, 43
 - by obscurity, 4, 95, 121
 - cost of, 8
 - home LAN, 241
 - host-based, 253–255
 - layered, 96
 - policy, 7–10, 13, 56, 177
 - public information, 119–120
 - strategies, 11–13
 - vs. convenience, xvii, 19
- security association, *see* SA
- security manager, **81**
- Security Parameter Index, *see* SPI
- security policy, **7**
 - sample, 215–216
- Security Policy Database, *see* SPD
- sed* (program), 219
- Seiden, Mark, 38
- self-defense, 17
- sendmail*
 - configuration, 43
 - DEBUG hole, 287, 288, 294
 - disabled by removing execute permission, 310
 - hard to configure, 43
 - most common mailer, 43
 - non-network security holes, 125, 298
 - SMTP front ends for, 43
- sendmail* (program), 126, 168, 267, 310, 312
- sendwhale, *see* *sendmail*
- sequence numbers, **22**, *see also* TCP, sequence numbers
 - attacks, 23, 29
 - initial, 23
 - vulnerabilities, 104
- serial lines, 181
- Server Management System, *see* SMS
- Server Message Block, *see* SMB
- Servers, **22**
- servers
 - NAS, 265
- services
 - anonymous FTP, *see* FTP, anonymous
 - small, **71–72**
- servlets, **82**
- session directory, **67–68**
- session ID, **324**

- Session Initiation Protocol, *see* SIP
- setgid, 125
- setuid, 123–125
- setuid* (program), 164, 168
- setuid*, 52, 298
- setuid *root* programs, **124–125**
 - list of possibly extraneous, 126
 - table of, 124
- setupsucker* (program), 297
- SGI, 264
 - Irix 6.2
 - inetd.conf*, 269
 - Irix systems, 264
 - setuid programs on, 124
- SGI MIPS
 - M/120, 290
- SHA, 327
- Shadow* (program), 159
- shadow password file, *see* passwords, shadow
- Shamir, Adi, 343
- shared libraries, 164
 - Apache uses, 165
 - modified to record password attempts, 128
 - modified with back doors, 127
- shell escapes, 64, 66
- shell script
 - created by *sendmail*, 293
 - generated by *httpd*, 66
 - hidden in `/usr/lib/term/.s`, 298
 - setupsucker*, 297
 - to simulate *login*, 295
- shim, 243
- Shimomura, Tsutomu, 64, 289, 296, 308
- shopping cart, **77**
- Shostack, Adam, 170
- shunning, **113**
- shutdown* (program), 126
- signature, digital, *see* digital signature
- Simple Authentication and Security Layer, *see* SASL
- Simple Mail Transfer Protocol, *see* SMTP
- Simple Network Management Protocol, *see* SNMP, *see* SNMP
- Simple Object Access Protocol, *see* SOAP
- Sinux
 - setuid programs on, 124
- SIP (Session Initiation Protocol), 46, **47**
 - filtering, 208
- site-local address, **35**
- skinny-dipping, 277
- Slackware, 261
- slapper* (program), 117, 171
- slashdot, 351
- SLASHDOT.ORG (host), 90
- sleep* (program), 290, 294
- SLIP, 126
- sliplogin* (program), 126
- smart cards, **147**, 150
 - attacks on, 147
 - can store biometric data, 148
 - handheld readers, 147
 - PC card readers, 147
- smart hub, 160
- SMB (Server Message Block), **57–58**, not
 - seesmb169*, 209
 - filtering, 209
 - passwords sniffed by *dsniff*, 129
- smb.conf* (file), 169
- smbd* (directory), 169
- smbd* (program), 169
- smptd* (program), 168
- SMS (Server Management System), 193
- SMTP (Simple Mail Transfer Protocol), **41–43**, 267
 - commands
 - DEBUG, 288, 290, 291
 - EXPN, 42
 - MAIL FROM, 42
 - RCPT TO, 288
 - VERFY, 42
 - doesn't have to run as *root*, 43
 - filtering, 203–204, 223
 - open relays, 204
 - over SSL on port 465 (deprecated), 171
 - passwords sniffed by *dsniff*, 129
 - sample session, 42
 - sample unfriendly session, 288
 - spoken by Web browsers, 74
 - wrapper, 43
- SMTP.ATT.COM (host), 32
- SMTSPS, 171
- smtps* (program), 224
- smurf, *see* attacks, Smurf
- SNA, xviii

- sniffers, **58**
- sniffing, 58–59
 - X11 magic cookies, 71
- sniffing attacks, xiii
- sniffing tools, 123
- SNMP (Simple Network Management Protocol), **62–63**, 326
 - authentication, **326**
 - community strings, **62**
 - common, 252
 - “public”, 63, 252
 - GET, 62
 - GETNEXT, 62
 - MIBS and, 62
 - monitoring network elements, 271
 - SET, 62
 - shut off, 265
 - TRAP, 62
 - version 1, **62–63**
 - version 3, **63**, 265, 271
- sntp* (program), 66
- snort*, 282–283
 - sample rules, 283
- snort* (program), 275, 282, 283, 351
- SOAP (Simple Object Access Protocol), 228, 235
 - tunneling with, 235
- social engineering, **98–100**, 122, **132**
 - with URLs, 78
- SOCKS, **187**
 - diagram of a typical connection, 187
 - passwords sniffed by *dsniff*, 129
- socks* (program), 90
- software
 - anti-virus, 106–107
 - evaluating, 155
 - loading and upgrading, 270
- software engineering, 102
- Software Engineering Notes*, 350
- software tools, **153–171**
 - network monitoring, **159–162**
- Solaris, 63
 - field stripping, 267
- SONET, 20
- Song, Dug, 129
- source routing
 - blocking, 183
- Southwestern Bell, 248
- space station, 67
- Spafford, Gene, 111
- spam, 14, 109, 223
 - filtering
 - with *postfix*, 168
- spamming, **108**
- SPARC, 266
- SPD (Security Policy Database), 320
- SPI (Security Parameter Index), 240, 318
- spiderweb, 19
- SPIGOT (host), 177
- spoofing
 - ARP, **22**, 34, 118, 160
 - backscatter and, 116–117
 - DNS, 32, 59, 330
 - easy with UDP, 27
 - firewall rules to prevent, 180
 - firewalls to prevent, 180
 - IP, 20, 116
 - IP source addresses, xiii, 48, 60, 71, 72, 104, 149, 156, 161
 - by ISP customers, 115
 - DOS attacks, 110
 - in DOS attacks, 107
 - mail addresses, 99
 - the current time, 337
 - tracing back, 114
 - UDP source ports, 207
- spoiling, needs disk space, 268
- sprintf* (program), 155
- spyware, **69**
- SQUEAMISH.CS.BIG.EDU (host), 32
- src/httpd* (program), 165
- Ssh* (program), 157
- ssh*, **61–62**
 - admin access to VPN device, 244
 - authentication shortcomings, 157–158
 - configuration, 61–62
 - cryptology of, **322–323**
 - cvs* and, 238
 - DSA authentication, 156
 - filtering, 206
 - on highly-secure hosts, 255
 - one-factor authentication, 154–156
 - problems with, 61–62
 - protocol 2, 154

- protocol failure with NFS, 105
- protocols, 61
- server authentication, 158
- tunneling IP packets over, 243
- tunneling X11, 71
- two-factor authentication, 157
- UsePrivilegeSeparation, 158
- Windows implementation *putty*, 61
- ssh* (program), 15, 39, 57, 59, 61, 62, 71, 105, 129, 154, 156–158, 188, 199, 203, 204, 206, 210, 219, 222, 238, 243, 244, 253, 255, 271, 274, 275, 277, 322, 323
- ssh-agent* (program), 61, 323
- ssh-keygen* (program), 156
- ssh_config* (file), 61
- sshd* (program), 61, 274
- sshd_config* (file), 61, 156
- sshmitm* (program), 158
- SSL (Secure Socket Layer), 10, 77
 - cryptology of, **323–325**
 - instant messaging, 46
 - other protocols over, 171
 - POP3 and, 45
 - protocol overview, 324–325
 - security, 325
 - version 2 enabled in shipped Web browsers, 83
 - Web browsers and, 77
 - with *sslwrap*, 170–171
- SSLtelnet* (program), 59
- sslwrap*, 170–171
- sslwrap* (program), 169–171
- Stacheldraht, 111
- stack-smashing, **100, 167**
 - IMAP server, 283
 - rpcbind*, 50
 - snort* can detect attempts, 282
 - in *fingerd*, 100
 - in *rstatd*, 123
 - in *syslog*, 158
 - in the shell *read* command, 88
 - not likely in Java, 210
 - weird hardware frustrates, 266
- stance, **9–10**, 188, 208
- Stanford University, 288, 289, 291–293, 296, 297
- Stazzone, Anthony, 42
- stdio* (program), 164
- stel* (program), 59
- stelnet* (program), 59
- stereotyped beginnings, 340
- Stevens, W. Richard, 19
- Stoll, Cliff, 159, 293
- Stornetta, W., 347
- Strategic Air Command, *see* SAC
- strcat* (program), 155
- strcpy* (program), 155
- stream cipher
 - used by WEP, 39
- Stream Control Transmission Protocol, *see* SCTP
- strings* (program), 127
- StrongARM, 244
- stub routines, 47
- stunnel* (program), 170
- su* (program), 96, 125, 265
- substitution box, *see* S-box
- subversion by route confusion, **183**
- suexec* (program), 165, 167
- sulfnbk.exe* (program), 100
- Sun, 220
 - setuid programs on, 124
- supercomputer, 7
- Sweden, 299
- Sybase SQL
 - passwords sniffed by *dsniff*, 129
- Symantec pcAnywhere
 - passwords sniffed by *dsniff*, 129
- Syslog* (program), 272
- syslog*, 158–159
 - Macintosh uses, 264
- syslog* (program), 126, 264
- syslogd* (program), 158
- System V
 - ps* command, 292
 - Release 4
 - mailer, 288
- tail -f* (program), 292
- talk* (program), 291
- tar* (program), 273
- targets of opportunity, 106, 262

- TCB (Trusted Computing Base), 102, 163, 261, 331
- TCP (Transmission Control Protocol), **22–24**
 - listen*, 22
 - acknowledgment number, 22
 - circuit gateways, *see* gateways, circuit level
 - close, 24
 - filtering, **202–203**, *see also* packet filtering
 - considerations, 178
 - policy discussion, 203
 - half-opened
 - hiding probes with, 122
 - half-opened connections, **23**
 - protocol change proposal, 116
 - SYN attacks and, 109
 - header bits
 - ACK, 178, 188, 207
 - RST, 178
 - hijacking, xiii, **59**
 - encryption defeats, 130
 - encryption prevents, 118
 - network monitors can promote, 160
 - of X11 sessions, 71
 - one-time passwords don't stop, 59
 - SASL alone doesn't prevent, 149
 - tools available, 71
 - tools for, 118
 - was theoretical, 130
 - logging, 187
 - open, **23–24**
 - initial sequence numbers, 23
 - SYN attacks and, 23
 - ports, *see* TCP ports
 - reliable delivery, 22
 - sequence number, 22, 104
 - attacks, **23**, 104, 118
 - DOS attacks and, 111
 - idiosyncratic, 111
 - initial, 23, 104
 - leaking, 71
 - predicting, 23
 - visualization of generation algorithms, 25
 - server ports, 22
 - servers, 22
 - session, 24
 - small services, **71–72**, 79
 - states
 - TIMEWAIT, 53
 - tunneling
 - with *ssh*, 61
 - with PPP, 235
 - won't continue a non-existent session, 178
 - wrappers, *see* TCP wrappers
- TCP ports, **22**
 - 113 (*identd*), 217
 - 137–139 (NetBIOS), 263
 - 143 (IMAP4), 283
 - 20 (FTP-data), 53, 103
 - 6000– (X11), 70
 - 80 (HTTP), 165
 - less than 1024, 23
 - privileged, **23**, 59
 - scanning, 106
- TCP wrappers, *see* wrappers
- TCP/IP, **19**
- TCPA (Trusted Computing Platform Alliance), 331
- tcpdump* (program), 123, 159, 214, 226, 275, 282, 295, 296, 407
- tcprelay* (program), 187
- tcptraceroute* (program), 160
- Telcordia, 146
- telecommuting, 234, **239–242**
- telephony, 46–47
- telnet*, **58–59**
 - over SSL on port 992, 171
 - passwords sniffed by *dsniff*, 129
- telnet* (program), xiii, 10, 54, 55, 58–60, 65, 113, 138, 144, 149, 182, 184, 187, 219, 230, 235, 271, 310, 312, 322
- telnetd*
 - back door in, 127
- telnetd* (program), 127
- telnets, 171
- TEMPEST, *see* electronic emissions
- Temporal Key Integrity Protocol, *see* TKIP
- Teredo, **37**
- terminal, xvii
- terminal server, 289
- terminology, xix
- Texas A&M University, 289
- TFN (Tribe Flood Network), 110
- TFTP (Trivial File Transfer Protocol), **52–53**

- blocked from outside at a university, 184
 - router configuration and, 53
- tftpd* (program), 98
- TGS (Ticket-Granting Server), 314–316
- thanks, xx
- The North American Network Operators' Group, *see* NANOG
- THEIRHOST (host), 178
- This is not a virus.exe (file), 207
- Thompson, Ken, 98, 99
- ticket, 315–317
 - Kerberos ticket-granting ticket, 317
 - ticket-granting, 315, 316
- Ticket-Granting Server, *see* TGS
- tiger teams, **132–133, 231**
- time* (program), 71
- time-to-live, *see* TTL
- timedc* (program), 126
- timestamp
 - based on *ntp*, 63
 - changing a file's, 63
 - digital, 347
 - Kerberos, 315
 - SNMP, 326
 - synchronizing logs, 63
 - useful in cryptographic protocols, 63
- timestamps, *see* cryptography, timestamps
- TIS, 211, *see* Trusted Information Systems
- TiVo, 274, 331
- TKIP (Temporal Key Integrity Protocol), **39–40**
 - WEP replaced by, 39
- TLS (Transport Layer Security), 323
- token, *see* authenticator, handheld, **145**
- tools
 - hacking, *see* hacking, tools
 - network administration, 160–162
- topology, 182
- traceroute6* (program), 126
- traceroute*, 160
- traceroute* (program), 21, 27, 30, 121, 160, 183, 209, 215, 217, 230, 280
- traceroute-as* (program), 31
- traffic
 - analysis, 186, 318, 320
 - incoming, 7
 - shaping, **220**
- transitive trust, **11, 13, 60, 179, 249**
- Transmission Control Protocol, *see* TCP
- transmission error, *see* error propagation
- Transport Layer Security, *see* TLS
- traps, *see* honeypots
- Tribe Flood Network, *see* TFN
- Trickey, Howard, 187
- Trinoo, 111
- trinoo*, *see* hacking tools, *trinoo*
- Tripwire* (program), 275
- trivestiture, xiii
- Trivial File Transfer Protocol, *see* TFTP
- Trojan
 - typographical errors, 123
- Trojan horse
 - in *OpenSSH*, 275
 - in released software, 275
- Tru64
 - setuid programs on, 124
- trust
 - asymmetric, 156
- trust graph, 327
- Trusted Computing Base, *see* TCB
- trusted computing base, 102
- trusted computing base,, 163
- Trusted Computing Platform Alliance, *see* TCPA
- trusted path, 11
- TTL (time-to-live), 160, *see* IP, TTL field
- tunnel, **233**
- tunneling, 66, 67, 234–236, 238
 - encrypted, 183
 - IP level, 319
 - IP over IP, 235
 - L2TP, 235
 - PPTP, 235
 - TCP with PPP, 235
 - through *ssh*, 243
 - UDP packets, 188
 - with SOAP, 235
- tunnels, **234–236**
 - bypassing firewalls, 235
 - diverting traffic through, 30
 - DNS and, 239
 - GRE, 30
 - IPsec
 - resists connection hijacking, 118
 - to access selected parts of intranets, 249
 - troubles on Windows hosts, 243

- TV, 291
- two-factor authentication, 137
 - in *ssh*, 157

- U.S. Navy, 261
- UDP (User Datagram Protocol), 27
 - ban outgoing packets, 208
 - easy to spoof, 27
 - echo service, 207
 - filtering, 207–208
 - no flow control, 27
 - packet storms, 72
 - RealAudio and, 68
 - safe filtering is hard, 207
 - small services, **71–72**
 - suitable for query/response applications, 27
 - tunneling, 188
- UDP ports
 - (32769–65535) Mbone, 67
 - 2049 (NFS), 52
 - 3544 (Teredo), 37
 - 53 (DNS), 170, 201
 - less than 1024, 23
 - Mbone, 67
 - multicast destinations, 67
 - random, 67
 - scanning, 106
 - spoofing, 207
 - syslog, 158
- ukase, *see* edict
- Ultrix, 302, 306, 310, 311
- Uniform Resource Locator, *see* URL
- uninterruptible power supply, *see* UPS
- University of Michigan, 275
- UNKNOWN.FLEEBLE.COM (host), 201
- upas* (program), 262
- UPS (uninterruptible power supply), 193
- Urban, M., *see* fonts, Tengwar
- Urban, Michael, 435
- URL (Uniform Resource Locator), 65, **78–79**
 - can be dangerous, 65
 - invasive, 79
 - on beer bottles, 3
- USENET, *see* netnews
- Usenix, 295
- UsePrivilegeSeparation, 428

- User Datagram Protocol, *see* UDP
- utmp
 - altering, 126
- utmp (file), 126, 127, 295–297
- utmpx (file), 126
- uucp* account, 125, 297
- uucp* program, 60, 98
- uucp* (account), 60
- uucp* (program), 60, 67

- Van Dyke, Jerry, 291
- Venema, Wietse, 64, 168, 262, 297, 299
- Verisign, 80
- version-rollback attacks, **45**
- virtual circuit, **20, 22**
- virtual private network, *see* VPN
- Virus construction kits, *see* hacking tools, Virus construction kits
- viruses, 17, **106–107**
 - anti-virus software, 106–107
 - checking, 206–207
 - IBM Christmas Card, 106
 - infecting stolen software with, 56
 - losing the arms race with, 331
 - scanning for, 263
 - spread by e-mail, 44
 - urban legends as, 106
- voice print, 147
- VPN (virtual private network), xv, 233, 236–242
 - address assignment problems, 239–241
 - as firewall, 258
 - DNSsec and, 239
 - for accessing past departmental firewalls, 257
 - in hardware, 244
 - in software, 243
 - susceptible to viruses and Trojans, 243
 - telecommuting with, 239–242
 - tunnels
 - replicated firewalls and, 192
 - used by joint ventures, 238
 - YourKey, 244
- VRRP
 - passwords sniffed by *dsniff*, 129

- w (program), 295

- W3C (World Wide Web Consortium), 235
- Wagner, David, 38, 159
- WAN, 320
- war dialing, 121, 248
- war drive, 242
- war driving, **38**
- warez, **56**, 349
- Warrell, C., xx
- weather forecasts, interrupted, 16
- Web, **73–91**
 - basic authentication, 85
 - digest authentication, 85
 - hijacking, 84
 - protocols, 74–77
 - search engines
 - finding hacking tools, 128
- Web browsers, 83–85
 - ActiveX and, 80
 - bypassing disabled JavaScript in, 83
 - FTP and, 77
 - have insecure ciphersuites enabled, 83
 - Java and, **80–82**
 - plugins, 264, 277
 - recommendations, 84–85
 - risks to, **79–85**
 - S/MIME in, 326
 - shipped with SSL ver. 2 enabled, 83
 - SSL and, 77
- Web bugs, **79**, 205
- web of mistrust, 111
- web of trust, 327
- Web proxy, **90**
- Web servers
 - access controls, **85**
 - Apache, 165–167
 - basic authentication, 85
 - choice of, 87–89
 - chroot environment, 66
 - database access by, 91
 - locating, 89–90
 - provisioning by users, 156
 - risks to, **85–87**
 - safe configuration, 165–166
 - sample of a very small one, 88
 - scripting, **86**
 - securing, 86–87
- Web services, 65–66
- WEP (Wired Equivalent Privacy), **38–40**, 318
 - protocol failure, 105
 - security flaws in, 38–39
 - TKIP replaced, 39
- WEPCrack (program), 39
- white box testing, 230
- WHITEHOUSE.COM (host), 78
- WHITEHOUSE.ORG (host), 78
- who (program), 126, 127, 295
- whois, **64–65**
 - whois (program), 64, 299
- WiFi, *see* 802.11
- Wilson, Norman, 167
- WILYHACKER.COM (host), 78
- Windows, 138, 175, 205, 243, 263
 - crashed by *nmap*, 130
 - file and printer sharing, 58
 - not suitable for high-security hosts, 255
 - percent found on intranets, 252
 - spyware on, 69
 - susceptible to worms, 206
 - target for virus writers, 106
 - tightening up, 263–264
 - troubles with IPsec, 243
- Windows 2000
 - Kerberos in, 313
- Windows 3.1, 263
- Windows 95, 263
- Windows NT, 138
 - as a TCB, 261
 - Lan Manager
 - weak authentication, 169
 - LanManager
 - dictionary attacks on, 138
- Windows XP
 - developer support for IPv6, 329
- Wired Equivalent Privacy, *see* WEP
- Wired magazine, 309
- wireless, **38–40**
 - base stations, 247, 265
 - contain firewalls, 175
 - find with war driving, 242
 - in the home, 239
- World Wide Web, *see* WWW
- World Wide Web Consortium, *see* W3C
- worms, **106–107**
 - blocking, 206–207

- Code Red, 87, 258
- creating Botnets, 117
- cross-platform, 106
- Love Bug, 243
- Melissa, 106, 205, 243, 253
- Morris, 11, 102, 112, 262
 - Orange Book would not have stopped, 102
- Nimda, 83, 87
- Slapper, 111
- spread by e-mail, 44
- wrappers
 - alternate TCP ports and, 171
 - CGI, 86, **166–167**
 - inetd*, 154
 - SMTP, 43
 - Xwrapper* for X11, 125
- wtmp* (file), 127
- wu-ftpd* (program), 167
- WWW (World Wide Web), 65, 66
 - query scripts, 66
- WWW.ALTAVISTA.COM (host), 78
- WWW.ALTAVISTA.DIGITAL.COM (host), 78
- WWW.APACHE.ORG (host), 165
- WWW.NATO.INT (host), 288
- WWW.PLAYGERBIL.COM (host), 79

- X Display Manager Control Protocol, *see* XDMCP
- X.25, 182
- X.CS.BIG.EDU. (host), 32
- X.TRUSTED.EDU (host), 199
- X11, **70–71**
 - call with *xwrapper*, 125
 - challenge/response security scheme, 71
 - filtering, 209
 - font library accessed through TFTP, 52
 - Kerberos version, 71
 - magic cookies, 71
 - must provide own authentication, 103
 - not handled well by packet filters, 188
 - passwords sniffed by *dsniff*, 129
 - terminals booted with TFTP, 52
 - ssh*, 71
 - tunneling
 - with *ssh*, 61, 71
 - with IPsec, 71
 - used to snatch passwords, 98
- X11* (program), 125
- xauth* (program), 71
- Xbreaky* (program), 270
- xdm*, **71**
- xdm* (program), 71
- XDMCP (X Display Manager Control Protocol), 71
- XDR (External Data Representation), 48
- xforward* (program), 188
- xhost* (program), 71
- xlogin* (program), 71
- XNS, xviii
- xterm* (program), 262
- XUNET project, 301
- Xwrapper* (program), 125
- xwrapper* (program), 433

- yacc* (program), 102
- Yellow Pages, **50**
- Ylönen, Tatu, 61
- YourKey VPN hardware, **244**
- YP, **50**
- YP/NIS
 - passwords sniffed by *dsniff*, 129
- ypchfn* (program), 126
- ypchpass* (program), 126
- ypchsh* (program), 126
- yppasswd* (program), 126

- Zalewski, Michal, 24
- zombies, **110**, 117
- Zonealarm* (program), 226