

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, file, account, and program names are generally indexed under the major categories “host”, “file”, etc.

- 10BaseT network, 129
- 2600 Magazine, 156
- 7ESS, 29

- A.2d, 199
- access control lists, **35**
- account
 - dummy, 140
 - expiration, 98
 - on gateways, 99
 - shutdown, 98
- accounts
 - Firstname.Lastname*, 11, 75
 - actual-user-name*, 115
 - adrian*, 168
 - anonymous*, 41, 101, 130, 184
 - beferd*, 171
 - berferd*, 133, 171, 176
 - bin*, 43, 111, 134, 154, 178
 - bugtraq-request*, 248
 - bugtraq*, 294
 - b*, 170, 171
 - ches*, 183
 - demo*, 140, 191
 - field*, 12
 - foo*, 134, 154
 - ftpmail*, 239
 - ftp*, 101, 103, 104, 130
 - guard*, 96, 97
 - guest*, 8, 12, 16, 133, 134, 138, 140, 149, 176, 184, 185, 191, 193
 - localuser*, 254
 - lp*, 149
 - majordomo*, 247
 - netlib*, 188
 - remoteuser*, 254
 - rfc-info*, 257
 - risks-request*, 248
 - rlogin.myhost*, 223
 - root*, 8, 14, 24, 30, 31, 38, 41, 43, 90, 101, 103, 108, 110, 111, 114, 119, 130, 139, 147, 152, 154, 155, 163, 168, 170, 173, 178, 183, 184, 223
 - sync*, 149, 184
 - sys*, 184
 - uucp*, 43, 92
 - visitor*, 140, 149, 191
- acorns, 181
- Address Resolution Protocol, *see* ARP
- address space probes, 137
- address-spoofing, *see* attacks, address-spoofing
- adjunct password file, *see* passwords, file, shadow
- Adleman, L, 218
- administration, xii, xiii, 8, 16, 26, 43, 45, 48, 85, 90, 110, 170, 176
- administrative domains, **53**
- Advanced Research Projects Agency, *see* DARPA
- AFS, **38**, 39

- authentication, 39
- alligators, 44
- Andrew File System, *see* AFS
- anonymous certificates, *see* certificates, anonymous
- anonymous FTP, *see* FTP, anonymous
- application gateway, 75–76
- ARP, **22**, 22
 - limited table size, 152
 - permanent entry for gateway router, 90
 - phony entry to block access, 91
 - proxy, 152
 - requests slow network scans, 146, 152
 - seed entries to detect address scan, 137
 - turn off processing on router, 91
 - use indicates an address scan, 191
- ARPA, **19**
- ARPANET, 19
- artificial intelligence, ridicule of, 110, 181
- ASCII, 29
- ASN.1, 35
- assurance of attack detection, 133
- assurance requirements, 8, 52, 162
- astronauts, 46
- asymmetric cryptosystems, *see* cryptography, public key
- Asynchronous Transfer Mode, *see* ATM
- AT&T, 11, 13, 17, 29, 31, 73, 88, 126, 160, 183, 191
 - Bell Laboratories, xii, 85, 186
 - Corporate Security, 143
- Atlantic Reporter, 199
- ATM, **20**, 69, 125
- attacks
 - active, 32, 48, 79, **213**
 - address scanning, 29
 - address space, 137, 152
 - address-spoofing, 24, 25, 34, 38, 45, 65–69, 72, 82, 93, 109, 123, 129, 141, 164, 235
 - birthday, **213**, 222
 - bogus NFS requests, 108
 - bogus NIS backup servers, 37
 - change file timestamps, 33
 - chosen-plaintext, **213**
 - code book, 215
 - come in groups, 137
 - connection laundering, 3, 45, 99, 113, 140, 142
 - connection laundering sites, 140
 - controlling inverse DNS tree, 28
 - cryptographic, 212, **213**
 - cut-and-paste, **213**
 - demon dialing, 145–147
 - denial-of-service, **30**, 82, 90, 128, 150, 162, 165–166
 - ICMP, 70
 - ICMP messages, 166
 - identd, 141
 - remove *portmapper* service, 35
 - syslog* port, 109
 - dictionary, 12, 14, 39, 43, 159, 167
 - DNS cache contamination, 28, 99
 - DNS zone transfers, 27
 - drop all connections with ICMP, 25
 - dumpster diving, 155
 - executable files in FTP area, 44
 - exhaustive search, 212, **213**, 214, 217
 - fetching `/etc/passwd`, 160
 - file name as shell command, 139
 - forged signatures, 233
 - guest accounts, 140
 - ICMP, 137
 - ICMP redirects, 150–152
 - inside, 11, 76, 77
 - IP source routing, 26, 67
 - Kerberos authenticators, 226
 - known-plaintext, **213**
 - laundering connections, 178
 - mail address-spoofing, 161
 - man-in-the-middle, **213**, 220
 - MBone packets through a packet filter, 46
 - name server, 94, 123
 - name-spoofing, 28, 43
 - network mapping, 147
 - network scans, 29
 - NFS-exported file systems, 149
 - NIS, 149
 - on Kerberos' initial ticket, 226
 - passive eavesdropping, 27, 154, 155, **213**
 - password logging, 155
 - password-guessing, 134, 154, 164, 236
 - ping, 146
 - port scanning, 150

- practical cryptanalysis, **213**
- protocol holes, 164
- recovering from, 155
- replay, **123**, **213**, 231
 - during clock skew, 120
 - foiled by different challenge, 121, 123
 - if IV is constant, 231
 - IVs prevent, 215
 - Kerberos authenticators, 226
 - Secure RPC prevents, 38
 - set back time, 33
- routing, 26, 27
- RPC services, 135, 149, 192
- scanning networks, 145
- searching for targets, 145
- sequence number, 24
- shell escapes, 101
- SNMP, 145
- social engineering, 155
- source routed packets, 150
- source-address-spoofing, 89
- sources of, 190–192
- spreading, 152
- subversion by route confusion, 72
- subverting routing with ICMP `Redirect`, 26
- TCP sequence number, 164
- temporary visitor account, 161
- through *guest* account, 8
- time-spoofing, 33, 109, **213**
- Trojan horse, 32, 33, 38, 42, 154, 155, 161, 191, 202, 239
- trusted hosts, 154
- via UDP multicast, 104
- auditing
 - concealing from, 33
 - programs, 244–246
 - TCP connections, 141
 - tools, *see* hacking, tools
 - via NFS, 107
 - with *SATAN*, 149
- authentication, **119**, 119–124
 - address-based, 24, 28, 47, 93, 109, **123**, 141, 164
 - address-based fails, 26
 - based on source address, 123
 - bidirectional, 224
 - BSD, **42**
 - by name, 37, 43
 - challenge/response, 108, 114, 120, 121, **121**, 122, 216, 221, 226, 235
 - X11, 48
 - cryptographic, 33, 119, 123–124, 236
 - database, 119, 120
 - evaluation, 117
 - failures, 163–164
 - for proxy use, 77
 - FTP, 159
 - hand-held, 96, 119
 - host-to-host, 123–124
 - implied by cryptography, 211
 - Kerberos, 8, 78, 211, 223–226
 - in AFS, 39
 - interrealm, 250
 - login, 96
 - machine-to-machine, 119
 - magic cookie, 48
 - name-based, 27–28, 123, **123**
 - network-based, 123
 - NFS, 37, 38
 - not provided by UDP, 25
 - of cleartext messages, 232
 - of evidence, 200, **201**, 202
 - one-time passwords, 116
 - OSPF, 27
 - other, 119
 - outgoing, 115
 - password, 96
 - passwords insufficient, 86
 - philosophy, 161
 - policy requires strong, 86
 - RPC, 34
 - server, 32, 96, 98, 114, 116, 121
 - sample, 98
 - TIS, 115
 - server *authd*, 138
 - site-supplied, 97
 - SNMP, 231
 - something you are, **119**
 - something you have, **119**, 121
 - something you know, **119**, 120, 121
 - strong, 81
 - tickets, 225
 - time-based, 33, 120, 216

- weak, 119
- X11, 163
- authenticator, **223**, 225
 - hand-held, 10, 32, **120**, 121–123, 165
 - algorithm in, 98
- authorization, 35, **119**
- automatic teller machine, 121

- backdoors, 8, 161–163
- backup
 - day 0, 90, 111
 - DNS servers, 27
 - encrypting tapes, 15
 - gateway files, 110–111
 - network links, 73
 - NIS servers, 37
- bastion host, **51**, 88, 93
- battlements, 8
- beast, *see* wild beast
- Bell Laboratories, *see* AT&T, Bell Laboratories
- Bellcore, 122
- Bellovin, D., v
- Bellovin, R., v
- Bellovin, S., 167, 175
- belt-and-suspenders, **69**, 88
- Berferd, xiv, 92, 139, 154, **171**, 167–179, 183, 192, 208
 - mother of, 179
 - origin of, 178–179
- bind*
 - version 4.9, 243
- bind* function, 31, 77
- biometrics, 122–123
- birthday paradox, **222**
- black-bag jobs, 4
- blaster, atom, 143
- Bottom Secret, 22
- brute force, *see* attacks, exhaustive search
- BSD, 85, 90, 91, 242
 - authentication, **42**
 - ps* command, 172
 - version of *ftpd*, 101
- BSDI
 - screend* for, 74
 - suitability for gateway use, 89
- bugs, 83, **162**, 161–163
 - in critical systems, 15
 - in FTP login, 101
 - in *ftpd*, 41
 - in gateway code, 82
 - in mail header processing, 83
 - in MIME processing, 31
 - in WWW file pointers, 44
 - large programs are buggy, 7
 - old ones aren't fixed, 9, 148
 - possible, in router, 6
 - programs are assumed to have, 7, 8
 - routers generate bogus ICMP messages, 152
 - sendmail*, 83
 - source routing, 72, 150
 - system, are not most common attack, 11
- bugtraq*, 248
- business records, **200**, 200–201

- cache, 225, 226, 232
- California, 198, 205
- Caller*ID, 206, **206**
- callsigns service*, 189
- Capstone, **214**
- CBC, 215, **215**, 216, 221, 231, 233
- CD-ROM, 179
- CERT, 73, 113, 142, 172, 205, 247
 - advisory, 7, 32, 75, 83, 104, 159, 161, 203
- Certificate Revocation List, *see* CRL
- certificates, **220**, 233
 - anonymous, **232**
 - expiration dates, 232
 - PGP, 233
- CFB, 216, **216**, 231
- challenge/response, *see* authentication, challenge/response
- Channel, English, *see* English Channel
- Chapman, B., 55, 62, 64
- checksum
 - in WWW file pointers, 44
 - IP, *see* IP, checksum
 - Kerberos message, 223
 - MAC, 221
- Cheswick, L. E. P. A., v, xiv
- Cheswick, W., 167
- chmod*, 41
- choke, 88, **88**

- chroot, 45, 48, 81, 101, 103, 107, 108, 113, 114, 116, 130, 131, 139, 176
- Cipher Block Chaining, *see* CBC
- Cipher Feedback, *see* CFB
- ciphertext, 212, **212**, 214–217
- circuit gateways, *see* gateway, circuit level
- Cisco Systems, 89, 91
- civil damages, 198
- client programs, **24**
 - specialized, 117
 - unmodified, 115
- Clipper, **214**
- clock, 32, 33, 224, 231
- clock skew limits, 226
- CNN, 169, 175
- code
 - cryptography, 246–247
 - firewalls, 240–243
 - network monitoring, 243–244
- Comer, D., 19
- common law, 202
- common-mode failure, 46, 67
- computer crime, 183, 198–200
- Computer Emergency Response Team, *see* CERT
- Computer Fraud and Abuse Act, 198
- Computer Underground Digest, 156
- configuration
 - ARP entries, 90
 - choke router, 91
 - disk space, 90
 - external hosts, 89–91
 - gateway menu, 100–101
 - guard service, 96–98
 - kernel, 89–90
 - mail, 95–96
 - message-of-the-day, 90
 - network provider's router, 109
 - network services, 90
 - packet filters, 150
 - router ARP, 91
 - router virtual terminals, 91
 - routes in the router, 91
 - routing, 90
 - swap space, 90
- connect, 77, 125, 127
- connection server, **125**
- consent, 204
- console, 111, 114
 - access, 89
 - local access only, 89
 - maintenance through, 97
 - router access, 91
- Continental law, **202**
- COPS, 154
- copyright law, 42
- corollary, 7
- corporate, 6
- costs, 52
- counterintelligence, 16, 133–135, 137–139, 193
- Court of Appeals, 204
- CPU, 122
- Credit Card Fraud Act, 208
- cribs, **213**
- CRL, **232**
- cryptanalysis, 4, 14, 212
 - differential, 217
- cryptography, 8, 14–15, 22, 33, 35, 44, 159, 161, 163, 164, 211–234, *see also* encryption
 - asymmetric, *see* cryptography, public key
 - block cipher, 214
 - cipher block chaining mode, 215
 - client keys, 225
 - conventional, 212, 217
 - digital signatures, 220–221
 - electronic code book mode, 214–215
 - encryption, *see* encryption
 - exponential key exchange, 219–220
 - not authenticated, 219
 - initialization vector, 215
 - key, **212**
 - key distribution systems, 219
 - key escrow, **214**
 - legal restrictions, 212, 218, 220, 221, 231, 246
 - master keys, **212**, 217, 223
 - modes of operation, 212, **214**, 214–216, 231
 - PEM, 232
 - multi-session keys, **223**
 - output feedback mode, 215–216
 - padding, 215
 - private keys, 36, 224
 - private-key, 212–217
 - protocols, 212

- timestamps in, 33
 - public key, 124, **218**, 217–219, 232
 - disadvantages, 218–219
 - secret key, *see* cryptography, private-key
 - secure hash functions, 221–222
 - session keys, **212**, 214, 217, 219, 223, 224, 226, 229
 - symmetric, *see* cryptography, private-key
 - timestamps, 222–223
 - on a document, 222
- cryptosystems, **211**
- csh*, 173
- cyberspace, 107

- D'Angelo, D., 167, 176
- DARPA, **19**
- DASS, 234
- data channel, **40**
- Data Encryption Standard, *see* encryption, DES
- database
 - key, 98
 - stored inside, 98
- datagram, **20**, 25, *see also* UDP
- Datakit
 - connection to gateway, 77
 - dialer, 125
 - doesn't support urgent pointer, 126
 - gateway implemented with, 88
 - research implementation, 88
- DCE, **35**
- DEC, *see* Digital Equipment Corporation
 - gateway software, 126
- Decision, 170–172, 174
- decryption, *see* cryptography
- demilitarized zone, *see* DMZ
- demise, 14
- demon dialing, **145**
- denial-of-service, *see* attacks, denial-of-service
 - exhausting disk space, 165
- Dept. of Justice, 203
- DES, 212–214
 - CBC mode, 231
 - certified for authentication, 214
 - modes of operation, 212
 - security of, 217
 - used by X11, 164
 - used to secure SNMP, 231
- dest**, 125
- device driver, **19**
- Dick Van Dyke show, 171
- dictionary attacks, **12**
- Diffie-Hellman, 35, **219**
- dig*, 145, 243
- Digital Equipment Corporation, 74, 75, 100, 106, 126
- digital signature, 220, **220**, *see* cryptography, digital signatures, 221
- Digital Signature Standard, *see* DSS
- digital timestamp, **222**
 - link value, **222**
 - linking, **222**
- directories
 - ..., 154
 - ..^T, 139
 - /usr/lib/term/.s, 302
 - /bin, 170, 173
 - /dev, 131, 176
 - /etc/named.d, 182
 - /usr/ftp, 43, 103
 - /usr/lib/term/.s, 178
 - /usr/local/boot, 39
 - /usr/spool/uucppublic, 43
 - /var/spool/mqueue, 31
 - bin, 43
 - X11 font library, 39
- discovery, **201**
- discrete logarithm, **219**
- diskless workstations, 39
- disks
 - hot spare, 110
- Distance Vector Multicast Routing Protocol, *see* DVMRP
- Distributed Computing Environment, *see* DCE
- dk, 77
- DMZ, **51**, 129
- DNS, **27**, 27–29
 - alias for FTP server, 61
 - backup servers, 27
 - block zone transfers, 72
 - bogus entries to detect hacking, 152
 - cache contamination, 28, 99
 - commands
 - forward, 62

- configuration, 86
 - controlling inverse tree, 28
 - corrupted entries, 137
 - cross-checks, 28, 43, 64, 139
 - dangerous misfeature, 28
 - dig* queries, 100, 130
 - evidence of hacker use, 137
 - external service, 61, 88
 - filtering, *see* packet filtering, DNS
 - gateway's resolution, 62
 - internal access, 61
 - internal and external access, 86
 - internal root, 62, 99
 - internal service, 62
 - internal service of external names, 62–64, 99
 - inverse mapping tree, 138, 139
 - inverse queries, 27, 29, 146
 - logging, 131, 137
 - permit UDP queries, 72
 - records
 - A, 28, 64
 - CNAME, 28
 - HINFO, 27, 28
 - HINFO, 147
 - MX, 27, 28, 76, 94, 255
 - NS, 28, 138
 - PTR, 27, 28, 64, 147
 - SOA, 28, 130, 138
 - rich source of target information, 29, 147, 165
 - secondary servers, 29
 - sequence number vulnerability, 164
 - shell scripts query, 243
 - tree structure, 27
 - unreachable root name servers, 99
 - used to tunnel, 80
 - wild-card records, 29
 - zone example, 61
 - zone transfers, 27, 29
- Domain Name System, *see* DNS
- dongle, *see* authenticator, hand-held
- drop-safe, *see* logging, drop-safe
- DS1, 74
- DSS, 220
- dumpster diving, 155
- Dutch law, 178
- DVMRP, 46, 104
- ECB, 214
- ECPA, 198, 202, 204
- edict, 6
- efficiency, 163
- eggs, 110
- Eindhoven University, 178
- Electronic Code Book, *see* ECB
- Electronic Communications Privacy Act, *see* ECPA
- electronic emissions, 4
- electronic mail, *see* mail
- elvish, *see* fonts, Tengwar
- email, *see* mail
- encapsulation, 46, 70, 79, 80
- encryption, 32, 79–81, 108, 236, *see also*
 - cryptography
 - telnet*, 229–231
 - application level, 229–234
 - block cipher, 214
 - DES, *see* DES
 - file, 3
 - first block, 215
 - key-id, 227
 - last block, 215
 - link level, 226–227
 - mail, 232–233
 - network level, 227–230
 - SNMP, 231
 - transport level, 227–229
 - triple, 217, 232, 233
- encryption, DES, 212
- English Channel, 15
- entrapment, 16
- environment variables
 - \$CALLER, 131, 140
 - \$DISPLAY, 104–106, 255
 - \$PATH, 38, 154
 - \$PROXY, 126
- erotica, 42, 139
- errata, xiv
- error propagation, 215, 216
- espionage, *see* industrial espionage
- Ethernet, 22
 - broadcasts ARP requests, 22

- cut transmit wire to, 175
- hide address from outside, 91
- monitoring packets on, 71, 137, 152
- monitoring with *tcpdump*, 175
- portmapper* designed for, 36
- promiscuous mode, 129, 137, 152
- tapping, 27
- ethics, 15–17
- evidence, 200–202
- exec*, 92
- expectation of privacy, 204
- expiration
 - accounts, 98
 - certificates, 232
 - key, 221
- exponential key exchange, 35, **219**, *see*
 - cryptography, exponential key exchange
- exponentiation, 218
- External Data Representation, *see* XDR

- F.2d, 199
- F. Supp, 199
- factoring, 218
- false statements, 198
- Family Educational Rights and Privacy Act, 207
- Farmer, D, 33
- FBI, 204
- FDDI, 20
- Federal interest computer, **198**
- Federal Reporter, 199
- Federal Rules of Evidence, **200**
- Federal Supplement, 199
- field, **219**
- file handle, 37, **37**, 38
- file systems
 - Andrew, 38–39
 - attacking exported, 149
 - attempted mount, 135
 - auditing, 182
 - checking integrity, 111
 - faking a full one, 140
 - FSP, 42
 - gopher shares with ftp, 107
 - incoming probes, 192
 - limited access on gateways, 48
 - prevent filling, 162
 - remote, 81, 107–108, 226
 - shared, 81
 - simulated, 176, *see also* jail partition
 - Truffles, 81
 - wiped out by hackers, 174
- File Transfer Protocol, *see* FTP
- files
 - .o, 131
 - .plan, 138
 - .project, 138
 - .rhosts, 31, 41, 43, 76, 99, 104, 118, 131, 140, 154, 155, 254
 - .sat, 149
 - README, 246
 - \$HOME/.rhosts, 43
 - /dist/internet.security/
 - firewall.book, xiv
 - /usr/include/rpcsvc/mount.h, 135
 - /dev/kmem, 31
 - /dev/log, 130, 131
 - /dev/null, 249
 - /dev/tty, 173
 - /etc/group, 182
 - /etc/hosts.allow, 92
 - /etc/hosts.deny, 92
 - /etc/hosts.equiv, 43, 154, 254
 - /etc/hosts, 174
 - /etc/inetd.conf, 90–93, 96, 99
 - /etc/motd, 90, 174
 - /etc/networks, 145
 - /etc/passwd, 12, 14, 37, 42, 43, 97, 104, 110, 114, 116, 148, 149, 154, 160, 181, 182, 184, 185
 - /etc/resolv.conf, 62
 - /etc/services, 93, 96, 98, 99
 - /etc/utmp, 138
 - /v/gate/guard, 98
 - /v/gate/serviced, 101
 - /v/gate/tcpd, 92
 - /v/lib/upas/smtpd, 92
 - ed.hup, 182
 - hosts.txt, 145, 183
 - inetd.conf, 172
 - resolv.conf, 63
 - stderr, 57
 - stdin, 147, 150

- stdout, 138, 150
- tech_tips/packet_filtering, 247
- utmp, 176
- filtering
 - letter bombs, 115
 - packet, *see* packet filtering
- filtering bridge, **129**
- finger, 33–34
 - alternatives to, 138
 - attack rates, 184–186
 - delivers false information, 16
 - distributes public keys, 233
 - generic, **133**
 - gets hole in, 161
 - kinds of use, 133–134
 - limited availability, 142
 - logging attempts, 16
 - maps names to email addresses, 34
 - provides cracking information, 165
 - provides hacking information, 30
 - reverse, 133, 134, 138, 140, 141, 242
 - safe_finger, 138
 - sanitized, 250
 - security test, 149
 - shut off on router, 91
 - tells source of logins, 150
 - varying formats, 142
- Finger, D., v
- fingerprint, 122, 123
- firewall, **9**, **51**, *see also* gateway
 - categories, 51
 - internal, 53
 - limitations of, 82–83
 - location, 53–54
- firewall-book@research.att.com, xiv
- Firewalls mailing list, 62, 247
- fonts
 - Hebrew *Hclassic*, 235
 - Tengwar, 11
- Foreign Corrupt Practices Act, **208**
- forward, 63
- Fourth Amendment, 204
- fragmentation, *see* packet filtering, fragmentation
- frame relay, 69
- France, 169
- fraudulent messages, 205
- Fremont, 147
- FSP, **42**
- FTP, **39**, 39–42, *see also* ftpd
 - /dev in anonymous area, 131
 - accounts
 - anonymous, 184
 - netlib, 184, 190
 - anonymous, 41, **41**, 44, 101–104, 107, 116, 139, 190, 193, 257
 - configuring, 103–104
 - internal server, 126
 - attacks on, 43, 149, 154, 184, 191
 - authentication for, 159
 - bogus passwd file, 12, 14, 139, 148, 160, 168, 170, 182, 184, 185
 - by email, 103
 - configuring, 11, 42, 44, 90, 165
 - control channel, 39, 57, 250
 - data channel, 57, 250
 - outbound connection, 60
 - denial-of-service with, 165
 - DES authenticated, 35
 - directory
 - clearing, 42
 - internal access to, 103
 - publicly writable, 42
 - updating by internal users, 111
 - exporting secrets with, 86
 - incoming, 42
 - laundering attacks, 45
 - logging, 139, 182
 - outbound service, 75, 94, 115
 - packet filtering, 57–60
 - performance through gateway, 115
 - proxy, 100, 126, 241
 - public files cleared daily, 139
 - requires calling address, 206
 - requires incoming calls, 77
 - sample usage, 239
 - security analysis, 113
 - services on gateway, 78, 88
 - software sites, 257
 - transfer modes
 - ASCII, 41
 - binary, 41
 - image, **41**
 - transfers, 139

- tunneling with, 80
 - use of TCP URGENT pointer, 126
- ftpd*
- bugs in login, 101
 - commands
 - PASV, 41, 59, 60
 - PORT, 40, 60
 - TYPE I, 41
 - USER, 40
 - MGET, 115
 - PASS, 163
 - PASV, 255
 - PORT, 94
 - USER, 163
 - configuring, 101–104, 118, 130
 - DNS cross-checking, 64
 - is too complex, 48
 - logging, 12, 130–131
 - modifications, 101–103, 130
 - privileges needed, 163
 - selecting version, 101
- Ganesan, R., 78
- garlic
- smb* likes, 167
- gas mask, 169
- gateway, **51**, 62, 76
- administrative access to, 111
 - application level, xii, **51**, 61, 69, 115, 125
 - evaluating, 117
 - application, requires internal root name
 - server, 99
 - belt-and-suspenders, 69
 - circuit, 61
 - circuit level, **51**, 69, 76–78, 88, 99, 127, *see also* tunneling
 - evaluating, 117
 - commercial, 116
 - configuration, 89–91
 - costs of a, 4
 - depends on correct router configuration, 6
 - design philosophy, 7
 - double host, 100
 - evaluating, 116–117
 - fail-safe design, 6
 - has professional administration, 10
 - internal, 51
 - leaks, 80
 - mail, 75
 - mistrust of, 10
 - packet filtering, 51, 76
 - performance, 95, 115
 - philosophy, 51–52
 - Plan A, 86, 88, 89
 - Plan B, 88, 89
 - Plan C, 88, 89, 93, 129
 - policy, *see* security, policy
 - proxy services, **76**, 99
 - and *tcp*, 115
 - configuring, 99
 - FTP, 100
 - library, *see* library, proxylib
 - library for, 100
 - listen with, 94
 - logging, 111
 - mosaic*, 107
 - NFS, *see* NFS, proxy
 - not in TIS toolkit, 115
 - proxy protocol, 126
 - sample connection, 77
 - security analysis, 113
 - statistics from, 189–190
 - X11, 106
 - relay services, 51, 76, 77, 93–94
 - configuring, 89
 - FTP, 61
 - improving performance, 115
 - login, 96, 97
 - mail, 61, 67, 80, 95
 - MBone, 113
 - netnews, 45
 - printer, 76
 - protect from network-level attacks, 82
 - proxy, 99
 - px11*, 106
 - xp11*, 106
 - socks*, *see* *socks*
 - UDP packets, 104
 - user-supplied, 117
 - X11 connections, 105
 - research, 133
 - risk analysis, 113–114
 - services, *see* services

- services menu, 97
- simple administration, 9
- single host, 100, 127
- single-machine, 86, 99, 115
- tools, *see* tools, gateway
- topology, 68, 69
- wrapper performance, 93
- Generic Security Service Application Program Interface, *see* GSS-API
- gethostbyaddr, 28, 139
- gethostbyname, 125
- gets, 161, 162
- Glick, P., 167, 176
- glue routines, 34
- GSS-API, **233**, 234
- guard, 96, 98, 113
 - installation, 96–98
 - program, 98
- Haber, S., 222
- hackers, **xiii**
 - are* out to get you, 162
 - attack on open communities, 52
 - attacking Stanford, 168
 - attacks, *see* attacks
 - attacks stimulates tool production, 169
 - average location, 187
 - Berferd, *see* Chapter 10
 - bulletin boards, 156
 - checklist, 154–155
 - detection of, 86
 - difficulty in tracing, 142
 - don't rely on DNS information, 165
 - Dutch, 178
 - go after log files first, 128
 - goals, 3, 152–154
 - hide login attempts, 130
 - hours, 187–188
 - launder connections through intermediate hosts, 142
 - lawsuits against, 202
 - legally untouchable, 178
 - like TCP port 87, 250
 - malicious, 4, 128, 154, 173–174
 - managing, 167
 - monitor Ethernets, 32
 - quality control, 14
 - remove logs first, 43
 - return to hacked machines, 142
 - share information, 191
 - tend to be impatient, 181
 - tools, 143–156
 - adjust file checksum, 112
 - automated, 143
 - availability, 143, 149
 - network monitoring, 129, 152, 175
 - use FSP, 42
 - want to see `/etc/inetd.conf`, 92
 - wipe file systems, 174
- hacking
 - tools, *see also* auditing, tools
- hand-held authenticator, *see* authenticator, hand-held
- Hansen, S., 168, 177
- hash2.0, *see* snefru
- HDLC, 228
- headhunters, 165
- hearsay, **200**, 202
- Hoffman, J., *see* fonts, Hebrew *Hclassic*
- home directory, 43
 - FTP writable, 41
 - of system accounts, 43
- honey pot, 130, **133**, 133–142, 150, 192
 - finger, 16
 - tools, 117
- host command, 147, 243
- host files, 137
- hosts
 - (OUTSIDE), 129
 - *.ATT.COM, 28
 - *, 55–57, 65, 67, 68, 72, 73, 109
 - .COM, 29
 - 1.2.3.4, 60
 - 127.0.0.1, 107, 109
 - 192.20.225.1, 137
 - 192.20.225.3, 27
 - 224.0.1.10, 252
 - 224.0.1.11, 252
 - 224.0.1.12, 252
 - 224.0.1.13, 252
 - 224.0.1.14, 252
 - 224.0.1.15, 252
 - 224.2.0.1, 252

- 224.2.1.1, 252
- 224.2.127.255, 252
- 224.8.8.8, 252
- 3.225.20.192.IN-ADDR.ARPA, 27
- 5.6.7.8, 60
- 7ESS.ATT.COM, 29
- A1, 229
- A2, 229
- A, 54
- B1, 229
- B2, 229
- B, 54, 229
- C, 54, 229
- D1, 229
- D2, 229
- E, 229
- F, 229
- GW, 63
- HOST A, 72
- HOST Z, 72
- INDNS, 63
- NET 100, 72
- NET 1, 67, 68, 71, 72
- NET 2, 66–68, 71
- NET 3, 66–68, 71
- NET 1, 53
- NET 2, 53
- ORG.DOMAIN, 11, 75
- ROUTER, 68
- UNKNOWN.BAR.COM, 64
- A.SOME.EDU, 30
- ACTUAL.DESTINATION, 115
- ADMINNET, 72
- BAR.COM.BIG.EDU, 28
- BAR.COM.DEPT.BIG.EDU, 28
- BAR.COM.EDU, 28
- BAR.COM, 28, 61
- CHOKE, 87–89, 91, 93, 95, 96, 98, 99, 101, 109, 114, 129
- CLIENT, 95
- COM.EDU, 29
- CSL.SRI.COM, 248
- DECWRL.DEC.COM, 239
- EMBEZZLE.STANFORD.EDU, 168, 170
- FC.NET, 248
- FOO.7ESS.ATT.COM, 29
- FOO.BAR.COM, 61
- FOO.BAR.EDU, 127
- FOO.COM, 25
- FOO.DEPT.BIG.EDU, 28
- FOO.EDU, 95
- FTP.CERT.ORG, 239
- FTP.RESEARCH.ATT.COM, xiv
- FTP.UU.NET, 239
- GREATCIRCLE.COM, 247
- GW, 66–68
- INET.ATT.COM, 30
- INET.RESEARCH.ATT.COM, 183
- INSIDE-NET, 73
- INSIDE, 87, 93–101, 109, 111, 113–115
- ISI.EDU, 257
- LOCAL-NET, 109
- MAILGATE, 73
- NIC.DDN.MIL, 34
- NINET.RESEARCH.ATT.COM, 27
- NTP.INSIDE, 72, 73
- NTP.OUTSIDE, 72, 73
- OUR-DNS, 72
- OUR-GW, 55, 65
- OURHOST, 56
- OUTSIDE, 87, 89, 93–101, 103, 105, 109–111, 114, 115
- PCLAB-NET, 72
- PSERVER, 93
- REMOTETHOST, 254
- RESEARCH.ATT.COM, 75, 134, 183
- RESEARCH, 95, 96, 113, 114
- RS.INTERNIC.NET, 34
- SECONDARY, 72, 73
- SPIGOT, 55, 65
- TARGETHOST, 150
- THEIRHOST, 56, 57
- X.TRUSTED.EDU, 61
- Hussein, Saddam, 168
- 1, 64
- IBM, 214
- ICMP, 25, 25–26
 - attacks
 - detected with *icmpmon*, 137
 - bogus messages, 152
 - can change routing, 25
 - denial-of-service with bogus packets, 166

- message contents, 25
- messages
 - Destination Unreachable**, 25, 141, 146, 150, 166, 252
 - Echo**, 130, 146, 147, *see also* ping
 - Port Invalid**, 70
 - Redirect**, 25, 26, 86, 91, 150–152
 - Time Exceeded**, 70
- old implementations drop all connections, 25
- raw socket, 152
- reports routing problems, 25
- routers can distinguish “safe” and “unsafe” packets, 70
- supplies port number, 141
- IDEA**, **214**, 214, 233
- identification, **119**
- Identification Friend or Foe, *see* IFF
- IETF**, **46**
 - meetings, 104
- IFF**, **121**
- IGMP**, **46**
- incident
 - Berferd, *see* Chapter 10
 - detection after the fact, 137
 - legal logs, 201
 - logging format, 127
 - rates, *see* Chapter 11
 - reporting, 130
 - scanning previous day’s, 110
- incoming
 - access policy, 74
 - access to port 2049, 38
 - calls, abuse, 77
 - file storage cleared, 42
 - filtering packets, 64
 - FTP**, 57
 - FTP** data connection, 41
 - FTP** directory, 42
 - login service, 88
 - logins, 96–98
 - mail, 28, 55, 61, 94–96, 250
 - mail policy, 75
 - mail service, 88
 - MBone** packets, 104
 - proxy use, 77
 - routing messages, 68
 - services, 78–79
 - socket, 126
 - telnet*, 96–98
 - telnet**, 61
 - telnet sessions, 48
 - viruses, 76
 - vs. outgoing TCP calls, 254
 - X11, 57, 60
- industrial espionage, 29, 30
- inet_ntoa**, 125
- inetd*, *see* tools, *inetd*
- information leakage, 165
- information protocols, **44**
- information security, 4
- information theory, **13**
- initialization vector, *see* IV
- insiders
 - access to gateway via NFS, 107
 - can export secrets with **ftp**, 75
 - rejecting a firewall, 80
 - risk from, 114
 - telnet** access to gateway, 103
- installation, *see* configuration
- integrity, 201
- integrity checking, 14
- internal gateway, **51**
- internal networks, 140
- internal users, *see* insiders
- Internet, 21
 - growth, 4, 5
 - shutdown incoming access, 74
- Internet Control Message Protocol, *see* ICMP
- Internet Engineering Task Force, *see* IETF
- Internet Group Management Protocol, **46**
- Internet Protocol, *see* IP
- Internet Relay Chat, *see* IRC
- Internet Security Scanner, **149**
- Internet Talk Radio, **104**
- Internet Worm, 30, 88, 161, 162, 198
- Iowa, permits printouts as evidence, 202
- IP**, **19**, 19–22
 - accounting, 189
 - addresses, 21
 - class D, 46
 - broadcast, **46**
 - checksum, 19, 20
 - configuration, 80

- connectivity, 85, 89, 235
 - conversion to “IPng”, 236
 - delivery isn’t guaranteed, 20
 - dialup, 235
 - encapsulation, 104
 - filtering fragments, 56
 - fragmentation, 20, **20**
 - from a portable computer, 237
 - header, 19, **19**, 20, 228
 - hops, **20**
 - host address, **21**
 - host can have multiple addresses, 24
 - IP-over-IP, 80
 - labels, *see* security, labels
 - multicast, **46**
 - group, 46, **46**
 - network address, **21**
 - options, 26, 67
 - over IP, 70
 - packets, **19**
 - routing, *see* routing
 - security labels constrain routing, 22
 - security option, 21
 - source routing, 26, 67, 69, 72, 86, 89, 116
 - loose, **26**
 - subnet address, **21**
 - tunneling, 80, 228
 - with DNS, 80
 - unicast, **46**
 - use numeric addresses, 93, 94, 99
 - use of bogus addresses internally, 73
- ipccopen, 126
- ipccpath, 126
- IPng, **236**
- Iraq, 168
- IRC, **156**, 252
- ISDN, 236
- ISS, 149
- IV, **215**, 216, 231
-
- Jacobson, Van, 147
- jail partition, 92, 175–179
- Jerusalem, 169
- joint ventures, 80–82
 - sharing file systems, 81
- Karlbridge, 74
- KDC, **123**, **212**
 - external, 225
 - for RIPEM, 233
 - must be available in real time, 218
 - safeguarding, 14
- Kerberos, 8, 39, 124, 223–226, 229, 231, 234
 - attacks on initial ticket, 226
 - authentication, 78, 211
 - authenticators, 226
 - connecting outside realm, 225
 - instance, **223**
 - interrealm authentication, 250
 - key distribution, 223
 - limitations of, 225–226
 - no hand-held authenticators for, 226
 - primary name, **223**
 - principal, **223**, 224
 - realm, **223**
 - ticket, **223**
 - ticket-granting ticket, 226
 - variant of X11, 48
- kernel
 - configuration, *see* configuration, kernel
 - configuring mbufs, 89
 - source code, 86
- key, 236
 - cache, 225
 - database, 36, 98, 121, 122
 - distribution, 14, 35, 48, 164, 223, 229, 232–234
 - Kerberos, 223
 - distribution problems, 48
 - expiration, 221
 - exponential exchange, 35
 - lifetime, 227
 - public, 233
 - RIPEM, 233
 - session, **35**
 - stealing, 213
 - validity of RIPEM, 233
- Key Distribution Center, *see* KDC
- keyboard, 47
- keyrings, **233**
- keystroke logging, *see* monitoring
- Klaus, C., 149

- knob-twisting, 184, 185
- labels, *see* security, labels
- Lamport, Leslie, 121
- LAN
 - commercial monitors, 128
 - misconfigured router on the gateway, 71
 - monitoring foiled by encryption, 236
 - monitoring gateway, 128
 - network encryption on, 229
 - policies for home, 235
- Latin, Medieval, 199
- Laugh-in, 29
- laundering connections, *see* attacks, connection
 - laundering
- law enforcement, xiii
- least privilege, **163**
- legal notation, 199
- legal restrictions to cryptography, 212, 231
- letter bombs, 115
- liability, 206–209
 - for harboring hackers, 52
- libel, 208
- library
 - compatibility, 242
 - cracklib*, 245
 - design of, 125
 - get host names, 28
 - information protocol (X39.50), 107
 - IPC, 77
 - logging, 127
 - modification to, 77
 - netlib*, 183
 - portable application, 117
 - proxy, 77, 100
 - proxilib*, 125–126
 - limitations, 126
 - selecting gateway for, 126
 - regular expression, 93
 - RPC, 135, 137
 - securelib*, 77, 240
 - obtaining, 240
 - security problems with shared, 131
 - shared, 77
 - shared have had security problems, 254
 - standard connection validation, 253
 - SunOS, 240
 - system cracking, 160
 - X11 font, 39
- Linux
 - has recent software, 242
 - has user-level NFS server, 242
 - suitability for gateway use, 89
- lip-print, 123
- listener service, System V, 252
- load average, 31
- lockpicking, 144
- logging, 3, 92–93, 98, 110, 113, 117, 127–128,
 - 130–131, 133–134
 - constant file format, 127
 - drop-safe, 88, **110**, 110
 - files, 181
 - finger attempts, 16
 - forged logs, 200
 - ftpd*, 130–131
 - guard connections, 97
 - in *ftpd*, 101
 - in *inetd*, 130
 - in *login*, 130
 - incidents, 127
 - incoming data, 133
 - inverse DNS queries, 131
 - legal concerns, 200–202
 - mail, 201
 - needs disk space, 90
 - noise, 192–193
 - proxy connections, 189
 - scanning, after-the-fact, 139
 - subroutine library, 127
 - syslog* LOG_INETD, 127
 - syslog* LOG_PROXY, 127
 - syslog* LOG_SMTPSCHED, 127
 - TCP destination, 77
 - TCP wrapper, 127
 - use of *syslog* local entries, 127
 - useful for the postmaster, 75
 - with *rpcinfo* command, 35
- login
 - authenticated, 88
 - banner, 203
 - guard, 121
 - logging improvements, 130
 - modifications, 131

- sample guard, 121
- logs, *see* logging
 - monitoring, 139
- loopback address, 109
- Los Alamos, 168
- loss of life, 15
- lures, *see* honey pot

- MAC, 221, **221**, 222, 224
- Macintosh, 127
- magic cookie, **47**, **164**
- mail, 11, 29–32, 45, 48, 67, 78, 79
 - aliases on gateway, 30
 - aliases provide hacking clues, 30
 - application gateway, 75
 - bastion host processing, 94
 - delivery, 67
 - delivery through a packet filter, 56
 - expertise at gateway, 30
 - fraud, 198
 - gateway, 75, 88
 - gateway security, 82
 - gateway transit time, 95
 - header lines, 83
 - headers, 30
 - incoming, 55, 75, 94–96
 - is most important network service, 41
 - logs, 201
 - mailing list, 30
 - may not be read by service providers, 205
 - multimedia, *see* MIME
 - outgoing, 94–96
 - postmaster, 201
 - return address not reliable, 30
 - serviced on gateway, 78
 - unused aliases, 149
- mailing list
 - firewalls*, 247
 - bugtraq*, 248
- mandatory access control, **22**
- manners, 15
- Markoff, J., 178
- MBone, **46**, 46–47, 70, 104, 113
 - gateway relay, 114
 - ports, 46
 - session directory, 104
- mbu.fs, the cereal of champions, 89
- MD2, 222, 232
- MD5, 222, 231–233
- media, xiii
- Merkle, R., 247
- Message Authentication Code, *see* MAC
- microphone, 123
- Middle East, 173
- military, 6
- milk, adulterated, 144
- MILTEN Spy, 204
- MIME, **31**, 31, 44, 107
- mine tunnels, 209
- minimal trust, **30**, 139
- MIPS
 - M/120, 115, 170
 - Magnum, 88, 89, 115
 - RISC/OS 4.52, 89
- MIT, 223
- mobile hosts, 79, 236
- modems, 235
- modes of operation, *see* cryptographic, modes of operation
- Mogul, J., 57
- monitoring, 32, 43, 48, 79, 128–129, 170, 175–177, 193, 202–206, 232
 - Ethernet, 137
 - illegal, 204
 - passwords, 159
 - random, may be illegal, 205
 - tools, 168
 - wiretap, 4, 12
- Morris, R. H., 161
- Morris, R.T., 198
- mount function, 107, 108
- mount daemon, 135, 192
- MS-DOS, xii, 128, 233
- multicast, 47, *see* IP, multicast
 - addresses, 104
 - audio, 104
 - backbone, *see* MBone
 - reception, 104
 - router support, 46
 - routers, 46
 - session directory, 46
- multilevel secure, **81**

- Multipurpose Internet Mail Extensions, *see* MIME
- Murphy's Law, 7
- Muuss, Mike, 148

- name service, *see also* DNS
 - attacks on, 123
 - bind* 4.9, 243
 - external, 62
 - internal, 62
- name serving
 - dumping the database, 145
- NASA, 46
- National Bureau of Standards, 214
- National Security Agency, *see* NSA
- NBS, *see* National Bureau of Standards
- NCR, 73
- negligence, *see* liability
- Netherlands, 178
- netlib*, 184
- netnews, **45**
 - defamation via, 208
 - on a gateway, 45
 - processing on the gateway, 45
 - resource hog, 45
 - security groups, 248
 - security holes in, 45
 - source of hacking software, 149
 - trusted sources, 48
- netstat*, 90
- network
 - backup links, 73
 - BSD-derived daemon, 85
 - disconnection not recommended, 6
 - external access, 100
 - hardening internal, 148
 - internal, 143
 - internal leaking outside, 145
 - modified daemons, 139
 - modified utilities, 126
 - standard management tools, 80
 - topology, 73
- Network File System, *see* NFS
- Network Information Service, *see* NIS
- Network Layer Security Protocol, *see* NLSP
- Network News Transfer Protocol, *see* NNTP

- network services
 - dragonmud, 189
- Network Time Protocol, *see* NTP
- New York Times*, 30, 178, 222
- newsgroups
 - alt.security*, 248
 - comp.risks*, 248
 - comp.security.announce*, 248
 - comp.security.misc*, 248
 - comp.security.unix*, 248
 - comp.sys.**, 248
 - comp.windows.x*, 248
 - misc.legal.computing*, 248
 - sci.crypt*, 248
 - proprietary, 45
 - security-related, 156
- NFS, **37**, 37–38
 - a more secure implementation, 81
 - blocked from outside at a university, 73
 - bogus requests, 108
 - detecting a hole with NOP, 193
 - disable on gateways, 90
 - file handle, 37, 107
 - is stateless, 37
 - Linux has user-level server, 242
 - mount daemon, 192, 193
 - proxy, 81, 107–108, 111, 126
 - public archives, 192
 - requests
 - NOP, 192, 193
 - root* access prohibited, 38
 - sample captured request, 192
 - sample proxy connection, 108
 - security of a archive site using, 191
 - suspicious access to, 70
 - used for auditing, 107
 - uses DES-authenticated RPC, 35
 - Version 2, 81
 - Version 3, 38, 81
- NIC, 145
- NIS, 14, **36**, 36–38, 149, 160, 164
 - disable on gateways, 90
- NIST, 214, *see* National Bureau of Standards, 220, 222
- NLSP, **227**, 228, 230
- NNTP, **45**, 45–46, 191
- North America, 187

- Northern Hemisphere, 187
- NSA, 161, 217
- NSFnet, 4
- NTP, **32**, 32–33, 70
 - installation, 109
 - permit access, 72
- numeric IP address, 125, 127, 145

- oak trees, 181
- OFB, 215, **215**, 216, 231
- onion, 82
 - ches* doesn't like, 167, *see also* garlic
 - glass, 82
- ooze, primordial, 209
- Open Shortest Path First, *see* OSPF
- Optimum Systems, 204
- Orange Book, **8**, 162
 - access controls, 8
 - auditing, 8
- OSF, 35
- OSI, 204, 227
- OSPF, **27**
 - authentication, 27
- outgoing
 - access policy, 74
 - authentication, 115
 - calls from high-numbered ports, 57
 - connections, 99
 - filtering packets, 64
 - FTP, 75, 115
 - FTP access, 94
 - FTP control requires incoming data
 - connection, 41
 - FTP data channel connection, 60
 - laundering calls, 3
 - mail, 94–96
 - mail headers, 30
 - MBone worries us, 113
 - packet filtering, 56
 - proxy, 189–190
 - restrictions, 3, 6
 - rlogin*, 115
 - secrets, 86
 - TCP proxy service, 77
 - TCP services, 99
 - telnet*, 100, 115
 - UDP packets, 70
 - vs. incoming TCP calls, 254
- output feedback mode, *see* OFB
- outside world, xii

- packet filtering, **51**, **55**, 54–75, 86, 91
 - AT&T policies, 235
 - better filter language, 254
 - block UDP port 2049, 38
 - blocking hosts, 96
 - bridge, 129
 - by subnet, 56
 - CERT recommendations, 247
 - compiler, 253
 - defense against port scanners, 150
 - distinguishing packet directions, 254
 - DNS, 57, 61–64, 72, 73, 250
 - erroneous, 55–56, 65, 66
 - evaluating, 116–117
 - fragmentation, 56–57
 - FTP, 57–60
 - high port numbers, 46
 - ICMP, 70
 - implementation, 74
 - IP fragmentation, 56
 - Karlbridge, 243
 - logging option, 254
 - MBone, 70, 104
 - MBone can subvert, 46
 - menu systems, 116
 - network provider, 109
 - on IP address, 243
 - on port number, 243
 - on regional network router, 109
 - other protocols, 70
 - outbound calls, 56
 - output only, 88
 - performance, 74
 - pinging through, 147
 - placement, 64–69
 - port summary, 249–252
 - portmapper*, 35, 64
 - preventing address-spoofing, 109
 - recommendations, 254
 - reject packets with options, 26
 - removed or erroneous, 6

- requires expertise, 55
- routing, 71–73, 80
- routing protocols, 254
- RPC, 64
- RPC requests hard to block, 192
- rule order, 66
- sample configurations, 73–74
- screend*, 242
- securelib, 240
- suppress ICMP Destination Unreachable, 25
- TCP considerations, 56
- testing, 150
- UDP, 69–70
- UDP is very hard, 69
- X11, 60–61
- XDR is hard, 35
- packet sucker, 133–135
- paranoia, 4, 6, 7, 36, 67, 69, 162
- `passwd` file, *see* `/etc/passwd`
- passwords, 11–14, 120, 122
 - why are you wasting your time*, 14
 - captured on logs, 183
 - converted to Kerberos key, 224
 - cracking, 14, 168, 226, 236
 - prevent with *cracklib*, 245
 - prevent with *passwd+*, 245
 - with *crack*, 149, 245
 - don't use conventional, 86, 245, 253
 - eliminate need for, 10
 - files
 - Berferd wanted to modify, 170
 - bogus, 12, 168
 - distributed by NIS, 36
 - in FTP directory, 42, 148
 - retrieval attempt rate, 192
 - shadow, 14, 37, 159
 - simulated for Berferd, 174
 - stealing, 160
 - stealing with *tftp*, 134
 - gateway administrative, 129
 - given out by NIS, 36
 - guessing, 11–12, 33, 34, 39, 143, 154, 164, 236
 - by Berferd, 167
 - over slow lines, 159
 - with *finger* information, 165
 - in encrypted *telnet*, 229
 - in exponential key exchange, 220
 - in log files, 130
 - in router configuration files, 39
 - keys generated from, 14
 - not reliable on tapped lines, 32
 - obvious, 140
 - on serial lines, 89
 - one-time, 32, 78, 96, 116, 120, 120–122, 216, 253
 - S/Key*, 241
 - optimum length, 13
 - poorly-chosen, 10
 - protect private keys, 164
 - protected by secure *telnet*, 32
 - protecting, 14
 - stealing, 12, 27, 32, 128, 129, 154, 155, 160–161
 - big-time, 77
 - by monitoring, 163
 - from the Ethernet, 236
 - with fake *login*, 153
 - with NIS, 149
 - stored on a gateway, 131
 - trafficking, 198
 - user-selected, 99
 - via NIS, 37
- PC, 24, 43, 73, 74, 76, 122, 127, 139, 141, 163, 191
- PCMCIA, 122
- PEM, 81, 232, 232–233
 - modes of operation, 232
- pen register, 202
- Pennsylvania, 206
- Perl script
 - generated by *httpd*, 45, 107
- personal identification number, *see* PIN
- personal use, 6
- pessimism, 8
- PGP, 232, 233
- philosophy, 55, 116
- phone book
 - determine organizational structure with, 165
 - network service, xi
 - on-line, 165
- phone-phreaking, 156
- Phrack*, 156

- physical perimeter, xi
- pigeons, 80
- PIN, 121, **121**, 122, 216
- ping*, 130
- pinglist*, 147
 - derived from *traceroute*, 147
- pirated software, 42
- plaintext, 212, **212**, 214–216, 218, 220
- Plan 9, 98, 113
 - authentication server, 98
- playback monitored terminal sessions, 178
- Point-to-Point Protocol, *see* PPP
- police, xiii
- politicians, 42
- port
 - above 1023, 57
 - high-numbered, 57
 - low-numbered, 57
 - privileged, *see* privileged ports
- port number, 24, 35, 36, 44, 47, 62, 64, 78, 125, 150, 255
 - incoming proxy, 94
 - random, 38, 46, 60, 64, 70, 135
 - range for *ftp* connections, 103
 - special login, 103
- portmapper*
 - forwards screened requests, 163
 - indirect calls, **35**
- postern gate, *see* backdoors
- postmaster
 - knows SMTP commands, 30
 - likes logging, 75
 - located with SMTP VRFY command, 30
 - logs have legal use, 201
- Postscript
 - can be dangerous, 31
- PPP, **80**, 235, 236
- Presotto, D., 88
- Pretty Good Privacy, *see* PGP
- prime numbers, 218
- print service, 76, 93, 94, 113, 114
- printouts
 - can be legal evidence, 200
- privacy, 15, 165, 207, 208, 232
- Privacy-Enhanced Electronic Mail, *see* PEM
- privileged ports, **24**, 34, 35
- programs
 - 3-D FS*, 77
 - COPS*, 154, 244, 246
 - Crack*, 149, 245, 246
 - Fremont*, 147, 244
 - ISS*, 149, 245
 - Karlbridge*, 243
 - MILTEN Spy*, 204
 - SATAN*, 149, 150, 245
 - SPI*, 246
 - S/Key*, 241
 - Swatch*, 139, 242
 - TAMU*, 244, 245
 - Telnet*, 31, 96, 97, 229
 - Toolkit*, 100
 - Tripwire*, 245
 - amd*, 192
 - archie*, 184
 - authd*, 138
 - awk*, 116, 127
 - bind*, 27, 243
 - bootp*, 149
 - cracklib*, 245
 - crontab*, 188
 - cron*, 43, 111, 139
 - dig*, 100, 130, 145, 147
 - domainname*, 134
 - emacs*, 193
 - etherfind*, 128
 - expect*, 149
 - expire*, 45
 - expose-me*, 153
 - fingerd*, 34, 149
 - finger*, 33, 34, 133–135, 138, 139, 160, 161, 165, 172, 184, 186, 233, 242, 250
 - fsirand*, 38
 - ftp*, 298
 - gopherd*, 45, 103, 107
 - gopher*, 44, 76
 - grep*, 77, 139
 - httpd*, 107
 - icmpmon*, 137, 138
 - ident*, 141, 241
 - inetd*, 31, 91, 92, 130, 134, 240, 254
 - insidetelnet*, 113
 - ipfilterd*, 74
 - ivs*, 252
 - lex*, 162

- login*, xi, 12, 31, 32, 94, 97, 101, 114, 130, 131, 140, 153, 154, 159, 176, 184, 254
- ls*, 38, 42, 161
- mail*, 62
- mount*, 107
- named*, 131
- netlib*, 183, 190
- netstat*, 176, 249
- nntpd*, 45
- nslookup*, 130, 243
- nv*, 252
- passwd +*, 245
- passwd*, 173, 245
- perl*, 107, 127
- pftp*, 126
- pinglist*, 147, 148
- ping*, 25, 70, 100, 130, 137, 146, 147, 152, 249
- port20*, 103, 131
- portmapper*, 35, 36, 38, 64, 135, 137, 138, 240
- portmopper*, 135, 136, 138, 188, 191
- potmapper*, 240
- proxyd*, 113
- proxynfs*, 113, 114
- proxy*, 113
- ps*, 172, 174, 176, 178, 249
- ptelnet*, 105, 126
- px11*, 105, 106
- rcp*, 193, 251
- rexecd*, 12
- rlogind*, 26, 43, 131, 254, 300
- rlogin*, 8, 10, 28, 42, 43, 72, 78, 96, 104, 110, 118, 121, 134, 171, 172, 183, 184, 191, 229, 241
- rm*, 15, 174
- routed*, 90
- rpc.mountd*, 107
- rpcinfo*, 35, 149
- rshd*, 26, 131, 254, 300
- rsh*, 41, 43, 57, 96, 134, 160, 163, 188, 193
- rusers*, 16, 138
- safe_finger*, 138, 287
- scanports*, 149, 150
- screend*, 57, 66, 74
- sd*, 252
- secrettelnet*, 113, 114
- securelib*, 77, 240
- sendmail*, 115
- seq*, 147
- serviced.sh*, 101
- setupsucker*, 176
- sleep*, 170, 173
- snefru*, 112, 222, 247
- socks*, 241
- sum*, 112
- su*, 12, 154
- syslogd*, 128, 131
- syslog*, 130
- systat*, 191, 249
- tail -f*, 172
- talk*, 171, 204
- tap*, 241
- tcpdump*, 128, 152, 175, 177, 286
- tcpmux*, 64, 193, 252
- tcpwrapper*, 240
- telnetd*, 94, 97, 101, 111, 131, 254
- telnet*, 16, 31, 32, 35, 43, 44, 48, 61, 71, 77, 78, 80, 88, 91, 94, 97, 100, 113, 114, 116, 120, 126, 131, 139, 140, 146, 150, 154, 160, 229, 231, 241, 242
- tftpd*, 14
- tftp*, 110, 160
- traceroute*, 70, 100, 130, 139, 145, 147
- tripwire*, 111, 246
- ttcp*, 115
- upas*, 31, 67, 92, 113
- uucp*, 43, 46
- uuencode*, 44, 76
- vat*, 252
- whois*, 33, 34, 178, 191, 250
- who*, 176
- w*, 176, 249
- xforward*, 241
- xgate*, 104, 105
- xmessage*, 105
- xmosaic*, 107, 115
- xp11*, 104–106
- xterm*, 105, 106, 138
- yacc*, 162
- ypx*, 149
- promiscuous mode, 71

- protocol
 - failures, 164
 - layers, **19**, 70, 82
 - should be visible to packet filters, 255
- proxy, **99**, *see also* gateway, proxy services
 - ARP, 91, **152**
 - NFS, *see* NFS, proxy
- proxymach, 126
- pseudo-random number generator, 38
- pseudo-tty, 101
- public key, *see* cryptography, public key
- Puddin'head Wilson, 110
- Pusan, S., xiv
- puzzle palace, *see* National Security Agency

- r*-commands, 42–44, 134
- random number generator, 215
- Rconnect, 127
- recommendations, 253
 - firewalls, 255
 - hosts, 253–254
 - protocols, 254–255
 - routers, 254
- recursion, *see* recursion
- regional network, 90, 109
- relay, *see* gateway, relay services
- reliability, 201
- Remote File System, *see* RFS
- Remote Procedure Call, *see* RPC
- replay attacks, **223**, *see also* attacks, replay
- Requests for Comments, **257**
- reservoir, dangers in owning, 209
- RFC, **257**
- RFS, **81**
- Rgethostbyname, 99
- RIP, **27**
- RIPEM, **232**, 233
- Risks Forum, 248, **248**
- Rivest, R, 218
- Riyadh, 172
- rlogind
 - modifications, 131
- rm -rf /*, 174
- roach motel, *see* jail partition
- router, **20**, 88, 89, 91, 96
 - established keyword, 96
 - access from console, 91
 - access to network provider's, 68
 - choke, 88, 91, 109
 - configuration, 54–75, 86, 90, 91, 94
 - configuration files, 39
 - deflecting routing attacks, 27
 - external, 91
 - IP accounting, 189
 - multicast support, 46
 - network provider's, 39
 - packet filtering, 55, 116
 - performance, 74
 - swamped by UDP packets, 25
- routing, 26–27, 235, *see also* packet filtering
 - asymmetric, **26**
 - attacks, *see* attacks, routing
 - configuration, 91
 - default route, 71, 90
 - filtering, *see* packet filtering, routing
 - ICMP can change, 25
 - leaks, 80
 - static, 90
 - subversion by route confusion, 72
 - trouble reporting with ICMP, 25
- Routing Information Protocol, *see* RIP
- RPC, **34**, 34–38
 - authentication, 34
 - cryptanalysis of Secure, 164
 - dump request, 135
 - filtering, *see* packet filtering, RPC
 - library, 135, 137
 - port scanners, 150
 - procedure number, **34**, 135
 - program number, **34**
 - secure, 48
 - sequence number, 34
 - sequence number vulnerability, 164
 - suspicious requests, 192
 - wrapper *Potmapper*, 240
 - wrapper *portmapper*, 135–137
 - X11 can use secure, 164
- RSA, **218**, 218
- RSAREF, 218, 233
- rshd
 - modifications, 131

- S/Key, 118, 122, **122**
 - obtaining, 241
- sacrificial host, 86
- satellite links, 227
- scanners
 - UDP, 150
- Scotland Yard, 15
- screend*, 242
- SCSI, 202
- Scuds, 169, 171
- SDNS, **227**
- SEAL, 75
- search warrants, 201
- Secure Data Network Systems, *see* SDNS
- secure hash function, 121, **221**, 231, 232
- secure hash functions, *see* cryptography, secure hash functions
- Secure RPC, **35**, 38, 48
 - key database, 36
 - problems with, 164
- security
 - “minimal trust” philosophy, 30
 - administrative domain, 53
 - belt-and-suspenders, 88
 - by obscurity, 85, 135
 - cost of, 4
 - definition, 3–4
 - domains, 53, **53**
 - labels, 21–22, 81
 - category, **21**
 - level, 21, 22
 - multilevel, 81
 - policy, **4**, 4–7, 9, 41, 53, 55, 197, 235
 - set by system administrators, 101
 - public information, 143
 - server, 78
 - strategies, 8–9
 - vs. convenience, xi, 19
- Security Analysis Tool for Auditing Networks, **149**
- Security Profile Inspector, **246**
- Seidlitz, 204, 205
- select**, 89, 94, 115
- self-defense, 16
- sendmail*
 - based letter bomb, 83
 - configuration, 30–31
 - DEBUG hole, 139, 167, 168, 174
 - disable on gateways, 90
 - distrust of, 67, 82
 - hard to configure, 30
 - most common mailer, 30
 - non-network security holes, 154, 178
 - recent bug, 83
 - SMTP fronts ends for, 31
 - we don’t trust, 113
- sendwhale, *see* *sendmail*
- sequence numbers, **22**, *see also* TCP, sequence numbers
 - attack, 24, **24**, 27
 - design recommendations, 255
 - initial, 24
 - vulnerabilities, 164
- serial lines, 20, 68, 89
- services, 94–109
 - anonymous FTP, *see* FTP, anonymous
 - gateway menu, 99–101
 - inbound
 - telnet*, 96–98
 - mail delivery, 94–96
 - MBone, *see* MBone
 - outbound
 - name service debugging, 100
 - network debugging, 100
 - ftp*, 100
 - telnet*, 100
 - outgoing TCP, 99
 - dig**, 100
 - ping**, 100
 - traceroute**, 100
 - proxy, *see* services, outgoing TCP
 - proxy NFS, 107–108
 - time, 109
 - WAIS, 107
 - WWW, 107
 - X11, 104–106
- session directory, 46, **46**
 - packets, 104
- setuid**, 38, 76, 90, 147, 153, 178
- SGI, 74
- shadow password file, *see* passwords, files, shadow
- Shamir, A, 218
- shell escape, **101**, 140

- in *rlogin*, 121
- shell script, 143, 150
 - created by *sendmail*, 173
 - delivered for *gopher* via FTP, 107
 - emulate *login*, 153
 - generated by *httpd*, 45, 107
 - guard*, 98
 - hidden in `/usr/lib/term/.s`, 178
 - provides gateway services, 100
 - scans for incidents, 181
 - setupsucker*, 176
 - to check file and directory integrity, 112
 - to simulate *login*, 176
 - uses *seq*, 147
- Shimomura, T., 168, 177
- shutdown, 94
- signature, digital, *see* digital signature
- Simple Mail Transport Protocol, *see* SMTP
- Simple Network Management Protocol, *see* SNMP
- Skipjack, **214**, 214
- smart cards, **122**, 122–124
 - hand-held readers, 122
 - PCMCIA readers, 122
- smart hub, 129
- SMTP, **29**, 29–31
 - can disclose hacking information, 146
 - commands
 - DEBUG, 168, 170, 171, 182
 - EXPN, 30
 - MAIL FROM, 30
 - RCPT TO, 168
 - VERFY, 16, 30
 - configuration, 92
 - doesn't have to run as *root*, 30
 - passing mail through a gateway, 95
 - relaying, 95
 - sample session, 29
 - sample unfriendly session, 168
 - security analysis, 113, 114
 - wrapper, 31, 115
 - in TIS toolkit, 241
- snefru*, 112
 - source, 247
- SNMP, **231**
 - access blocked by regional networks, 138, 145
 - authentication, 231
 - monitoring packages, 244
 - often not available on hosts, 138
 - probes were benign, 191
 - provides useful hacking information, 145
- SO_REUSEADDR, 103
- social engineering, **155**, **160**, 160–161
- socket, 77, 125
- socks, **77**, 127
 - in single machine gateway, 99
 - modified clients widely available for, 107
 - modifying clients for, 77
 - needs access to external name service, 99
 - obtaining, 241
 - uses numeric IP address, 76
- software engineering, 162
- Software Engineering Notes*, 248
- source address logger, 206
- source code
 - analysis of, 86
 - for daemons available via FTP, 130
- source-routed packets, 114
- spider web, 19
- spooling, needs disk space, 90
- stance, **6**, 60, 70, 77, 85, 88
- Stanford University, 168, 171–173, 177, 178, 209
- stateless servers, **37**
- stereotyped beginnings, 215
- Stevens, W. R., 19
- Stoll, C., 142, 173
- Stornetta, W., 222
- stub routines, **34**
- subnet address, 21
- subversion by route confusion, **72**
- Sun
 - portmapper*, 64
 - SunOS, 240
 - SunOS network monitoring tools, 128
- supercomputer, 3
- surveillance, 204
- swap space, 90
- Sweden, 179
- swIPe, **229**
- syslog*, 127–128
 - added to *fpd*, 101
 - added to local daemons, 130

- block external access to, 109
 - consistent logging format, 127
 - may listen on UDP port, 128
 - modifications to, 131
 - modify to use UNIX-domain socket, 131
 - sends log to drop-safe, 110
- syslogd*
- P option, 131
 - enhanced version in TIS toolkit, 139
- System V
- listener service, 252
 - MLS, 22
 - ps* command, 172
 - Release 3
 - listener service, 252
 - Release 4
 - mailer, 31, 168
- T.J. Hooper*, 207, **207**, 208
- TAMU, 74
- TCB, 162
- TCP, **22**, 22–25
- acknowledgement number, **22**
 - circuit gateways, *see* gateway, circuit level
 - encryption with NLSP, 227–229
 - filtering, *see* packet filtering
 - filtering considerations, 56
 - half-closed connections, 94
 - half-open connection, 24
 - header bits
 - ACK, 23, 56, 69, 96
 - FIN, 23
 - RST, 56
 - SYN, 23
 - incoming call for *ftp*, 94
 - listen, **24**
 - listen with *inetd*, *see* *inetd*
 - listen with *proxy*, 94
 - listening port
 - half open, 24
 - logging, 77
 - NFS over, 81
 - open request, 23
 - outgoing, 99
 - packet sucker, 134
 - port number, 24, **24**
 - ports, *see* TCP ports
 - proxy service, 77
 - relay, 82
 - reliable delivery, 22
 - sequence number, 22, 164
 - attack, 164
 - initial, 23, 24, 164
 - server ports, 24
 - servers, **24**
 - service for unserviced packets, 254
 - services on different interfaces, 86
 - shutdown, 94
 - states
 - TIMEWAIT, 40
 - synchronize bit, *see* TCP, header bits, SYN
 - tracing connections, 141
 - tunneling, 81, 82, 95
 - with PPP, 80
 - with TIS toolkit, 116
 - URGENT pointer, 94, 126
 - won't continue of non-existent session, 56
 - wrapper, *see* TCP wrapper
- TCP ports, *see also* Appendix B
- 515 (printer), 93
 - 6000–6100, 60, 104
 - privileged, 43
 - scan with *ISS*, 149
 - scanning, 150, 165
- TCP wrapper, **92**, 91–94, 96, 99, 101, 103, 109, 111, 113, 114, 130
- blocking TFTP, 118
 - logging, 97, 127
 - obtaining, 240
 - TIS, 115
 - Wietse Venema, 240
- TCP/IP, **19**
- tcpdump*, 243
 - telephones, 15
 - telnet*, 31–32
 - telnetd*, *see* tools, *telnetd*
 - TEMPEST, *see* electronic emissions
 - terminal, xi
 - terminal server, 168
 - terminology, xiii
 - Texas A&M University, 169
- TFTP, **39**
- blocked from outside at a university, 73

- TGS, **223**, 224, 225
- thanks, xiv
- The Cuckoo's Egg, **208**
- theft, 198
- theorem, 7
- Thompson, Ken, 161
- ticket, 224–226
 - Kerberos ticket-granting ticket, 226
 - ticket-granting, 224, **224**, 225
- Ticket-Granting Server, *see* TGS
- tiger teams, **148**, 155–156, 236
- timestamp
 - based on *ntp*, 33
 - changing a file's, 33
 - digital, 222
 - digital, service, 201
 - DNS information, 147
 - Kerberos, 224
 - SNMP, 231
 - useful in cryptographic protocols, 33
- timestamps, *see* cryptography, timestamps
- tin roof, 181
- TIS, 100, 115, *see* Trusted Information Systems
 - gateway software, 126
- TIS Firewall Toolkit, **115**, *see* tools, TIS toolkit
- TLSP, **227**, 228
 - TCP virtual circuits, 227
- token, **96**, *see* authenticator, hand-held
- tools
 - inetd*, 91–92
 - authd*, 138, 141
 - gateway, 91–94, 125–131
 - host scanning, 150
 - identd*
 - obtaining, 241
 - inetd*
 - logging improvements, 130
 - ISS, 149
 - network administration, 130
 - network monitoring, 128
 - network sweeps, 148–150
 - port scanning, 150
 - relay, *see also* gateway, relay services, 93–94
 - telnetd, 94
 - TIS toolkit, 44, 98, 115–116, 139, 241
 - obtaining, 241
 - wiretapping, 152
- Top Secret, 22
- Top-Level Certifying Authority, **232**
- topology, 71, 80
- tort, *see* liability
- traceroute*, 130, 148, 243
- tracing, 141–142
- trade secrets, **202**
- traffic
 - analysis, 76, **226**, 228
 - incoming, 6
- transitive trust, 8, 9, 43, 48, 54, **54**, 67
- transmission error, *see* error propagation
- Transport Control Protocol, *see* TCP
- Transport Layer Security Protocol, *see* TLSP
- trap and trace device, **202**, 205, **206**
- traps, *see* honey pot
- Trickey, H., 88
- Trivial File Transport Protocol, *see* TFTP
- Trojan horses, *see* attacks, Trojan horse
- Truffles, **81**
- trust, 10, 48, 53
- trust graph, 233
- Trusted Information Systems, *see* TIS
- trusted path, 8
- tugboat, *see* T.J. Hooper
- tunneling, 45, **79**, 79–80
 - encrypted, 73, 255
 - gateways should support, 255
 - implement joint ventures, 81
 - IP level, 228
 - TCP with PPP, 80
 - to a shared machine, 81
 - UDP packets, 78
- TV, 171
- U.S.C., 199
- UDP, **25**, 25
 - pinglist* use of, 147
 - traceroute* use of, 130
 - ban outgoing packets, 70
 - easy to spoof, 25
 - echo* service, 70
 - filtering, *see* packet filtering, UDP
 - no flow control, 25, 42
 - packet sucker, 134, 135

- port scanners, 150
- safe filtering is hard, 69
- sending *syslog* messages, 131
- service for unserviced packets, 254
- suitable for query/response applications, 25
- tunneling, 78
- UDP ports, *see also* Appendix B
 - 2049 (NFS), 38
 - 21 (FSP), 42
 - 53 (DNS), 62
 - forgery, 70
 - MBone, 46
 - proxy NFS, 107
 - remap MBone, 104
 - scanning, 165
 - syslog, 128
- ukase, *see* edict
- umask, 101, 103
- United States Code, **199**
- UNIX
 - philosophy, 125, 143
 - Tenth Edition connection server, 125
 - tools, 127, 153, 181
- Urban, M., *see* fonts, Tengwar
- USENET, *see* netnews
- Usenix, 175, 183
- user agents, **83**
- User Datagram Protocol, *see* UDP
- uucp* account, 111, 154, 178
- uucp* program, 43, 75, 95, 160

- Van Dyke, Jerry, 171
- vendor recommendations, 130–131
- Venema, W., 33, 115, 178, 179, 240
- video, 86
- virtual circuit, **20, 22, 76**
- virtual terminal, 91
- viruses, 16
 - infecting stolen software with, 42
 - scan for, 76
- voice conversations, legally protected, 205
- voiceprint, 122

- WAIS, **44**
- WAN, 229

- warez, 42
- Wargames dialing, **145**
- Warrell, C., xiv
- weather service, 189
- weather forecasts, interrupted, 15
- web of trust, 233
- webster service, 189
- Weinberger, P., 108
- whois*, **34, 145**
- Wide Area Information Servers, *see* WAIS
- wild beast, 208
- Wilson, N., 108
- wire fraud, 198
- wiretaps, *see* monitoring
- World Wide Web, *see* WWW
- WORM, 201
- worm, *see* Internet Worm
- WWW, 44, **44, 45**
 - file pointer, 44
 - file pointer checksum, 44
 - pointer, 44
 - query scripts, 45

- X.25, 69, 142
- X11, 47–48
 - can use DES-authenticated RPC, 35
 - can use secure RPC, 164
 - challenge/response security scheme, 48
 - DES authentication mode, 164
 - filtering, *see* packet filtering, X11
 - font library accessed through TFTP, 39
 - is dangerous, 106
 - Kerberos version, 48
 - must provide own authentication, 163
 - not handled well by packet filters, 57
 - protocol has vulnerabilities, 163–164
 - proxy
 - with *xforward*, 241
 - requires incoming calls, 77
 - terminals booted with TFTP, 39
 - through the gateway, 104–106
 - tools are often not simpler, 253
 - used to snatch passwords, 160
 - using *xforward*, 106
 - window managers are a special risk, 61
- XDR, **35**

xforward

obtaining, 241

xforward, 106

xgate, 104

xp11, 104

Yellow Pages, **36**

YP, **36**

ypx, 149

Z39.50, 107

zone transfers, 131, 138, 243