

# Index

- i3, 190
  - Shortcuts, 192
- 3G, 241, 274
  
- AAAA, 79, 181
- Access router, 214
- Accountability, 11
- Accounting, 240
- ACK, 60
- ACL, 176
- ACTIVE state, 76
- Address family, 248
- Address of record, 260, 263
- Address translation, 164, 218
- ADSL, 230
- Anchor point, 207
- Anonymity, 248
- Anti-replay window, 67, 72
- API, 47, 244
  - Native, 245, 246
- Applications, 113, 227
  - Legacy, 243
- Architecture, 5
- ASM, 98
- Attack, 208
- Attacks, 51, 176
- Attribute, 251
- Authentication, 11, 207, 230, 263
- Authentication server, 101
- Authorization, 11
  
- Base exchange, 51, 78, 85, 107, 179, 268
- Base64 encoding, 186
- Battery, 113
- BEET, 64, 164, 218
- Bidding down attack, 48
- BLIND, 218
- Boeing, 234
- Bootstrap, 87
- BOS, 87
- Break-before-make, 238
- Broadcast, 91
- Brute force, 15
- BTNS, 50
  
- Business model, 103
- Byte order, 246
  
- CBA, 69, 76
- Cellular, 69
- CERT, 229
- Certificate, 103, 179, 211, 239
- Channel binding, 243
- Charging, 240
- Checksum, 5, 52, 163, 167, 231
- Chord, 197, 273
- Churn, 184
- CLOSE, 61
- Collision resistant, 23
- Collisions, 48, 102, 164, 218, 223
- Compression, 260
- Confidentiality, 11
- Congestion control, 77
- connect() call, 243
- Consistency, 11
- Context establishment, 251, 256
- Cookie, 109
- Counter, 48
- CPU, 108
- Credit-based authentication, 76, 112
- Critical parameter, 74
- Cross-family handovers, 231
- Crypto Session, 266
  
- Data integrity, 11
- Data model, 96
- Delay attacks, 14
- Delegation, 210
- Demultiplexing, 165
- Denial-of-Service, 262
- DEPRECATED state, 75
- Designated router, 99
- DH, 19
- DHCP, 4, 183, 211
- DHT, 184, 219, 245
  - HIP interface, 186
  - OpenDHT, 185
  - Overview, 184
- Diagnostic, 273
- Diffie–Hellman, 19, 54, 107, 219

- DNS, 204
  - Extensions, 79
  - Secure, 40
- DNS query, 80
- DNSSEC, 45, 81, 182, 245, 260
  - Example, 41
- Domain, 204
- DoS, xvii, 7, 14, 76, 179, 190, 196, 219, 273
- Double jump, 67, 174, 200
- DR, 99
- Drowning attack, 186
- DSA, 46
- Dual stack, 6, 101
- Duplicate acknowledgments, 76
- Dynamic DNS, 188
  
- Eavesdropping, 13, 229
- ECHO\_REQUEST, 57
- ECHO\_RESPONSE, 68
- ED, 246
- Encryption, 111
- Endpoint descriptor, 246
- Ephemeral ports, 168
- ESP, 49, 62, 87, 95, 110, 163, 192, 244, 269
  - Anti-replay, 71
- ESP\_INFO, 63, 68
- ESP\_TRANSFORM, 63
- Exhaustive key space search, 15
- Extension headers, 165
  
- Failover, 76
- Fate sharing, 73
- Firewall, 90, 165, 175, 228, 234, 273
  - HIP-aware, 176
  - Legacy, 163
- First-hop router, 101
- Flags, 52
- Flow binding, 94
- Flow identification, 176
- Flow identifier, 93
- FON, 229
- Forwarding agent, 221
- FQDN, 79, 181, 244, 246
- FreeBSD, 280
- FROM, 79, 171
- FROM\_NAT, 167
- FTP, 243
- Fully Qualified Domain Name, 54
  
- getaddrinfo(), 249
- getlocalinfo(), 250
- getpeerinfo(), 250
- getsockopt(), 251
- GGSN, 276
- GPL, 279
- Group ID, 249
- GRUU, 261, 263
  
- Hairpin translation, 166
- Handover, 112, 205, 209
- Hash chain, 25, 206, 207, 224
- Hashed Message Authentication Code, 23
- HI blocking attack, 148
- HI stealing attack, 148
- Hi3, 190
- Hierarchy, 206
- HIP
  - Base protocol, 51
  - Benefits, 236
  - Extensions, 10
  - History, 7
  - Opportunistic, 177
  - Generalized, 255
- HIP\_SIGNATURE, 54
- HIP\_TRANSFORM, 54
- hipconf, 281
- hipd, 281
- HIPL, 279
- HISM, 99
- HIT, 46, 78, 86, 88, 99, 164, 188, 200, 220, 243, 256, 261, 275
- HMAC, 23, 57, 207, 268
- Hole punching, 166
- Host identity, 4, 239
  - Changing, 223
- Host Identity Specific multicast, 99
- HOST\_ID, 54
- hosts.allow, 228
- Hourglass model, 5
- HTTP, 165
- Hypervisor, 237
  
- I1, 51, 87, 168, 195, 220, 244
- I1\_SENT, 90
- I2, 57, 86, 221
- IANA, 47
- ICE, 166, 194, 264
- ICMP, 57, 61, 110
- Identifier, 4, 191, 256, 263
- Identifier-locator split, 4
- Idle security association, 64
- IETF, 7, 49, 258, 265
- IGMP, 99
- IKE, 37, 218
- IKE-H, 269
- IKE\_SA\_AUTH, 270
- IKE\_SA\_INIT, 269
- IKEv2, 37, 256, 269
- IMAP, 92
- Impersonation, 13
- Implementation, xvii, 279
- IMS, 241
- Indirection, 255
- Initiator, 51, 175, 197
- Inner address, 65
- Installation, 281

- Interface, 221, 243
  - Selection, 241
- Internet, 47
  - Sharing, 229
- Internet tablet, 105, 234
- Interoperation
  - IPv4 and IPv6, 230
- Intranet, 227
- INVITE, 260
- IP address, 166, 221
- IP options, 65
- IPsec, 49, 62, 64, 214, 263
- IPv4, 164, 276
- IPv6, 99, 212, 231
- ISP, 103, 188
  
- Keep-alive packets, 167, 174
- Kernel, 106, 281
- Key distribution, 104
- Key escrow, 240
- Key generation, 107
- Key size, 107
- Key splitting, 208
- Keying material, 28, 220
  
- Late binding, 256
- Lawful interception, 240
- LDAP, 233
- Leap-of-faith, 39, 85, 260
- Legacy application, 80
- Legacy hosts, 100, 184, 274
- LHIP, 117
- Lifetime, 200
- Lightweight hardware, 105
- Lightweight HIP, 117, 222
- Linux, 106, 279
- LOCATOR, 69, 74, 92, 175
- Locator, 4, 67
  - States, 75
- Locator lifetime, 75
- Locator management, 256
- Locator pair, 251
- Locator type, 75
- LRVS, 203
- LSI, 47, 188, 232, 245
  
- MAC, 23, 218, 222
- Man-In-The-Middle attack, 13, 80, 86
- Master key identifier, 268
- Maximum transmission unit, 46
- MCOP, 98, 100
- Measurements, 106
- Merkle–Damgård construction, 23
- Message authentication code, 23
- Micromobility, 203
- Middlebox, 208
  - HIP aware, 175
  - Legacy, 163
  - Middlebox traversal, 183
- Migration, 237
- MIP, 272
- Mipshop, 50
- MLD, 99
- MOBIKE, 49
- Mobile IP, 48, 49, 210, 256, 263, 274
- Mobile router, 211
- Mobility, 67, 183, 190, 204, 244, 275
- Mobility update, 112
- MODP, 28, 54
- Modular Exponential Diffie–Hellman Groups, 28
- Moskowitz, Robert, 8
- MTU, 77
- Multicast, 96, 197
  - Authentication, 103
  - Session identifier, 99
  - Mobility, 98
- Multihoming, 67, 69, 93, 211
  
- N770, 105
- Name resolution, 10, 181
- Name Space Research Group, 8
- Namespace, 45, 191
- NAT, 65, 164, 211, 224
  - Legacy, 163, 166
  - Mobility, 174
- NAT traversal, 258
  - Headers, 167
  - Initiator, 168
  - Responder, 170
- NEMO, 213
- Network mobility, 50, 197, 210
- Network operator, 240
- NIC, 7
- Nikander Pekka, 8
- Nokia, 234
- Non-repudiation, 11
- Nonce, 26
- NOTIFY, 60, 85, 173, 268
- NSIS, 176
  
- OASIS, 185
- OCALA, 277
- One-time signatures, 25
- One-way cryptographic hash functions, 23
- OpenDHT, 185, 239
- OpenGroup, 233, 234
- OpenHIP, 239, 279
- OpenWrt, 230
- Opportunistic mode, 52, 85, 188, 244, 245
- ORCHID, 47, 275
- Outer address, 65
- Overlay, 48, 98, 191
  
- P2P, 229
- P2PSIP, 259
- Packet reordering, 76
- Padding, 16

- Parameters, 54
- Path exploration, 251
- PDA, 105
- PEM, 249
- Perfect forward secrecy, 20
- Performance, 105, 240
- PF\_KEYv2, 65
- PF.SHIM, 246
- PFS, 20
- PGP, 5
- PIDF, 95
- Piggybacking, 86
- PIM, 99
- PIN, 241
- PISA, 229
- PKI, 5, 22, 233, 264
- PlanetLab, 185
- Policy, 267
- Port numbers, 223
- Port ranges, 94
- Porting, 106
- POSIX, 252
- Power consumption, 113
- Preferred locator, 71
- Prefix, 4, 46
- Presence, 96
- Prime factorization, 21
- Privacy, 11, 183, 217
- Private key, 247
- Private trigger, 190
- Protocol independent multicast, 99
- Protocol number, 52
- Protocol stack, 5
- Proxy, 262, 274
- Pseudoheader, 5, 231
- Pseudonym, 222
- Public IP address, 171
- Public key, 46, 219, 224
- Public Key Infrastructure, 22
- Public trigger, 190
- Public-key cryptography, 19
- Puzzle, 27, 54, 108, 174
  
- QoS, 92
  
- R1, 54, 169, 195, 220
- R1\_COUNTER, 57
- R2, 57, 86, 172, 221
- RADIUS, 233
- Referral, 243, 261
- REG\_FAILED, 82, 84
- REG\_INFO, 82, 88, 91
- REG\_REQUEST, 82
- REG\_REQUIRED, 82
- REG\_RESPONSE, 82
- Registrar, 83
- Registration, 78, 82, 170, 176
- Registration authority, 233
  
- Rekeying, 64, 215, 270
- Reliability, 11
- Remote subscription, 98
- Rendezvous, 9, 78, 96, 165, 177, 190, 203, 273, 275
- Replay attacks, 14
- Resolver, 248
- Resource record, 40, 80
- Responder, 51, 175, 220, 265
- Retransmission, 52, 188
- Return routability test, 259
- Reverse DNS, 221
- Reverse lookup, 183, 244
- RFC, 7
- RFID, 233
- Rivest, Shamir Adelman, 21
- Road Warrior, 227
- Rollover counter, 266
- Router, 100
- Routing, 4, 163
- Routing asymmetry, 176
- RPC, 185
- rpm, 281
- RRSIG, 40
- RSA, 21, 46
- RTT, 76, 86, 109, 185, 214
  - Estimation, 77
- RVA, 221
- RVS\_HMAC, 79
  
- S/MIME, 260, 264
- Salt, 267
- SCADA, 234
- Scratchbox, 106
- SCTP, 92
- SDP, 264
- Second preimage resistant, 23
- Security association, 49, 169, 275
- SEQ, 60
- Sequence number, 26, 222
- Service announcement, 88
- Service discovery, 87
  - On-the-path, 88
  - Passive, 90
  - Regional, 91
- Service distribution function, 195
- Service provider, 91
- Session establishment, 260
- Session mobility, 261
- Session report, 100
- setsockopt(), 251
- SHA, 219, 223
- SHIM layer, 250
- Shim6, 50, 259
- shim\_locator, 252
- SID, 99
- Side channel attack, 15
- SIGMA, 258

- Signature, 91, 177
  - Verification, 108
- SIM, 234, 241
- SIMA, 91
- SIMA\_ACK, 94
- SIMPLE, 95
- Single sign-on, 228
- SIP, 9, 241, 259
  - Presence extensions, 95
- Skype, 240
- SMA, 232
- Socket address, 248
- Socket attributes, 250
- Soft state, 101
- Source IP address, 193
- Source port, 170
- SPI, 64, 92, 175, 193, 222, 256
- SPI-NAT, 175, 191
- SPINAT, 217, 221
- SPKI, 103, 179
- Spoofing, 45, 172
- Spurious timeout, 77
- SRTP, 265
- SSH, 49
- SSM, 98
- SSRC, 265
- State, 176
- State machine, 57
- Stream cipher, 18
- STUN, 166, 256
- Suffix, 245
- Symmetric cryptography, 15
- SYN, 7, 86
- SYN-ACK, 86
  
- TCP, 5, 57, 77, 86
  - Option, 86
  - Port, 92
  - Port numbers, 87
- Throughput, 111
- Time-to-Live, 188
- Timeout, 170, 251
- TLS, 262
  
- TLV, 258
- Traffic type, 74
- Transform, 29, 250, 265
- Transport layer, 92
- Transport protocols, 6, 76
- Trapdoor function, 19
- Tree reconstruction, 101
- Triangle routing, 172
- Triggers, 250
- TTL, 90
- Tunneling, 101, 166
- Type-length encoding, 258
  
- UDP, 94, 164, 202, 228
- Unlinkability, 222
- UNVERIFIED state, 75
- UPDATE, 60, 82, 88, 92, 112, 174, 178, 199, 208, 211, 217, 239, 263, 266
- URI, 259
- User Agent, 95, 260
- User mobility, 261
- User-to-user communication, 259
- UUID, 95, 96
  
- Version Independent Group Management Protocol, 100
  
- VIA, 79
- VIA\_RVS, 169
- VIA\_RVS\_NAT, 174
- VIGMP, 100
- Virtual Machine, 237
  - Monitor, 237
- VPN, 227, 234
  
- Wireshark, 52
- WLAN, 106, 212, 229, 233, 276
- WPA, 111
  
- Xen, 237, 238
- XFRM, 65
- XML
  - Presence format, 95