

Index

- .NET, 11
- abstract simulation, 203
- Access Control, 72, 229
- Access Control List, 72
- Accountable Subgroup Multisignature, 75
- ActiveX, 118, 122, 123, 128, 130, 132
- ad hoc network, 2
- Adaptive Random Pre-distributed Scheme, 91, 93, 94, 102
- AgES, 41
- aggregated signature scheme, 87
- anthropomorphic metaphors, 8
- API call interception, 172
- API-SPY, 177
- AppScan, 191
- ASM, 76, 84
- attack flows, 149, 150, 166
- attack surface, 118
- Attack Surface Metric, 126
- Attack Vectors, 126
- attackability, 109, 111, 112, 125, 134, 135
- automated declassification, 205, 207
- backward recovery, 202
- BAN logic, 8
- BEAGLE, 2, 170
- bijection, 33
- binding update, 15–17
- bitwise binary addition, 53
- Bleichenbacher attack, 56
- block coding, 255
- bouncer, 2, 71, 73
- browser exploits, 1
- buffer overflow, 172
- Buffer Overrun, 116, 121, 126, 175
- CAGES, 41
- Cardholder Information Security Program, 188
- Certified AgES protocol, 40
- Certified Hash Protocol, 40
- certified hash protocol, 39
- CHP, 41
- CLIQUES, 64
- Code Red, 132
- code walker, 212, 213
- collude-then-spoof attack, 32
- colluding attacks, 42–45
- colluding spoofing attack, 36
- collusion attacks, 246
- commutative encryption, 33
- computation power, 148
- Consequential Cost, 142
- constant rate attack, 161
- Control State Corruption, 170
- Cqual tool, 203
- crawling process, 197
- cross-site scripting, 183
- CRT (Chinese Remainder Theorem), 83
- cryptographic, 1, 2, 9, 10, 14, 16, 17, 20, 22, 26, 30, 36, 40, 47, 51, 52, 54, 56–60, 71, 72, 75, 76, 78, 83, 86, 231, 232, 246, 251, 252
- cryptosystem, 51
- CSP, 12
- CTTPP, 41
- cyber-terrorism, 1
- cyber-war, 1
- D-WARD, 150
- data compression, 255
- data entry point, 192
- data integrity, 17
- data ownership certificate, 25
- DDoS, 147, 148, 166
- DDoS defense scheme, 147, 151
- DDoS detection algorithms, 147
- deep injection mechanism, 194
- Dennig-based systems, 202
- DER-encoded form, 81
- detection algorithm, 150
- Detours, 172
- DIDUCE, 178
- Diffie-Hellman, 53
- Diffie-Hellman Key Agreement Protocols, 66
- Diffie-Hellman key exchange scheme, 92
- digital signature, 229
- Directed Acyclic Graph, 246

- Distributed Intrusion Detection System, 140
- Document Object Model, 196
- Dolev-Yao model, 9
- DoS, 140, 148
- downstream routers, 149
- dynamic link library, 127

- encrypted key exchange, 62
- encryption key, 231
- error resilience, 230
- Eschenauer's scheme, 99, 100
- ESP, 203, 204, 220
- event-generation process, 197
- exclusive-or, 53
- exhaustive search algorithm, 62
- exhaustive search attack, 31

- false negative, 150
- false positive, 150
- Fault Triggering, 178
- FDR, 12
- finer-grained monitoring, 172
- fingerprint, 139
- Finite State Automata, 177
- flooding attack, 15
- flow-sensitive, 203
- forward recovery, 202
- functional queries, 48

- GAC protocol, 81
- GMC, 75, 77, 81, 83, 84, 87
- Gnutella protocol, 80, 81
- gradual pulsing attack, 161
- group charter, 73
- group signature scheme, 87
- GSM, 14
- guess-then-spoof attack, 32
- guessing attack, 32

- hash chain, 248
- hash function, 229
- hash protocol, 35
- hiding attack, 32
- Hippocratic Database, 36
- HMAC, 40
- Hoare, 201, 202
- Homomorphic DOC, 40
- Howard's Relative Attack Surface Quotient, 109
- HP, 41

- Identification Capability, 139
- identity theft, 1
- identity-based cryptography, 92
- IDS, 139
- IHSTC, 260
- image compression, 229
- Immunix Secured Linux, 199
- Import Address Table, 177
- increasing rate attack, 161
- information security system, 189
- information warfare, 148
- initiator, 29
- injection knowledge base, 194
- Injection Knowledge Manager, 197
- instrument library, 175
- instrumented semantics, 201
- integrating security services, 81
- Internet core routers, 149
- Internet Infrastructure, 148
- Internet-wide authentication framework, 149
- Intrusion Detection System, 2, 189
- ISAPI filters, 118, 127
- ITS4, 204, 205

- Javascripts, 197
- JIF, 199
- JPEG2000, 2, 229
- JPIP, 238
- JPSEC, 229

- key agreement, 2, 61–64, 67, 92, 104
- key agreement protocols, 55, 62, 92
- key decision algorithm, 97
- key distribution, 2, 91
- key insertion attack, 8
- key management, 20, 71, 72, 81, 93
- key selection algorithm, 94
- key transmission, 250

- lattice model, 201
- lattice-based, 200
- layer-increment, 232
- link overloading attack, 161
- listing queries, 48
- location authentication, 17
- lockdown instructions, 126
- Longest Common Subsequence, 173
- lossy compression, 231
- low-rate attacks, 150
- lowe's attack, 8

- malicious model, 41
- malicious pattern, 194, 217
- man-in-the-middle attack, 14
- master secret, 54
- MC, 204, 205
- MD5, 39, 63, 253
- merkle hash tree, 240
- message authentication, 16, 17
- message digest, 241
- message-passing, 117, 124
- metacompilation, 204
- Mobile IPv6, 8
- modulo a large composite, 65
- MOPS, 177

- Multics Intrusion Detection and Alerting System, 140
- mutual authentication, 15, 61, 62, 64, 93, 97, 102
- Needham-Schroeder, 8, 53
- negative response extraction, 194
- Network Anomaly Detection and Intrusion Reporter, 140
- network congestion, 147, 149, 150, 153, 154, 156
- Network Security Monitor, 140
- Next-Generation Intrusion Detection Expert System, 140
- niquely Assigned One-way Hash Function Scheme, 93, 102
- noninterference policies, 190
- NP-complete, 57
- Null session, 128
- observation period, 151
- one-way collision resistant hash function, 33
- one-way hash function, 240
- online privacy, 1
- Open Web Application Security Project, 188
- OpenSSL, 75, 76, 89
- P2P, 71–73, 75, 76, 79, 80, 87, 89
- packets, 235
- Password-only authenticated key agreement, 61
- peak signal to noise ratio, 260
- peer authentication, 71
- Peer Group Communication, 72
- peer-to-peer, 2, 11, 71, 72, 88, 89, 92
- PenaltyPeriod, 156
- penetration testing, 191
- phishing, 1
- PHP, 206
- PKC, 77, 81
- PKCS #1 protocol, 56
- PKCS7-formatted, 81
- plaintext, 33, 38, 56, 259
- power function, 33
- pre-distribute communication keys, 92
- precinct, 232
- precondition, 207, 211, 212
- Private Information Retrieval, 47
- private matching, 2, 25
- program abstractor, 211, 212
- proof-carrying codes, 200
- protocol analysis, 8, 9, 12, 19, 22, 51, 55, 56, 58, 60
- public key, 12, 14, 17, 23, 33, 38, 39, 47, 53, 59, 60, 74, 77, 88, 243, 246
- public key certificates, 61, 63, 241
- pulsing attack, 161
- Pushdown Automata, 177
- quality layer, 232
- Random Graph Theory, 93, 96, 102
- Random-Pairwise keys distribution scheme, 101
- random-pairwise scheme, 100, 101
- regular spoofing attacks, 36
- relative attack surface, 2
- Relative Attack Surface Quotient, 110
- remote procedure call, 127
- replay attack, 15
- resolution-increment, 232
- resource-driven security protocol, 92
- Robustness Testing, 178
- Rough Auditing Tool, 205
- RPC connections, 119
- RSA, 31, 56, 58, 67, 75, 76, 83, 84, 87, 145, 231
- sanity check, 132
- ScanDo, 191
- script injection, 183
- SECRET INFORMATION HIDING, 255
- secure admission control, 80
- secure IP tunnel, 16
- secure multi-party computation, 26
- Secure Spread, 72, 73, 79, 81, 82, 86
- Security Auditor, 142
- security automata, 200
- self-certification, 2
- self-certified, 62
- semi-honesty, 26
- semibundle, 57
- seminal key-agreement protocol, 55
- sensitive function, 207, 211, 214
- service quality, 148
- session key, 12, 14, 62, 64, 65, 92, 96
- set-homomorphic signature, 41
- SHA-1, 39, 63, 76, 84
- software testing, 183
- software verification, 184
- Software Wrapper, 170
- sophisticated detection strategies, 150
- source-end DDoS defense, 147
- SPIN, 92
- spoofing attack, 32
- Spread API, 82
- SRI, 57
- SSL, 54
- Stackguard, 199
- state machine, 112
- static group access control, 81
- static invariant, 209
- static most restrictive, 208, 209, 211
- static verification, 198
- switching-tree coding, 255.
- Sybil attacks, 81
- symbolic debugging, 22
- symmetric encryption, 52–54

- symmetric key, 249
- system authority, 63

- TCP SYN flooding attack, 161
- TFN2K, 148
- third party publication scenario, 238
- three-party EKE protocols, 62
- threshold encryption, 55
- throttling component, 151
- TOCTTOU, 204
- trace-based analysis, 13
- traceback techniques, 149
- Tribal Flood Network, 148
- Trinoo, 148
- Trojan horse, 140
- trusted third party, 35, 42, 44, 47, 92
- Trusted Third Party Protocol, 38, 39, 42
- trusted third party protocol, 35, 45
- TS-DSA, 75, 83, 84, 86
- TS-RSA, 75, 83, 84, 86
- TTPP, 41
- type guards, 203
- type inferencing, 208
- type judgments, 208
- type polymorphism, 203
- type qualifier, 199, 201, 203, 207, 212, 221
- type-aware qualifiers, 205
- typed assembly languages, 200
- typestate, 200, 203, 204, 208, 209, 212, 216, 226

- Uniquely Assigned One-way Hash Function Scheme, 91, 94, 102

- validation procedures, 194, 197, 217
- vector quantization, 255
- verification engine, 212
- victim network, 148, 149
- victim-end systems, 149
- Virtual Directories, 127
- virus, 1, 140
- voice compression, 255
- voice recognition, 255

- watermarking, 2
- Web Application Security via Static Analysis and Runtime Inspection, 183
- Web Application Vulnerability and Error Scanner, 183
- Web Security Scanner, 191
- webcrawler, 192
- WebInspect, 191
- WebSSARI, 183, 200, 205–207, 209–211, 213, 215, 216
- wide area group communication system, 81
- Wireless Sensor Network, 2, 91
- worm, 1, 132
- WSS, 191, 192, 215–218

- X.509, 77, 84, 88
- XML, 241