

Index

A

- abortive release (TCP) 304
- access (system call) 157–158
- access attributes 130
- access bracket 147–150
- access control 3, 6, 126, 134, 142, 195, 202, 214, 257, 282, 298
 - ... capabilities list (C-list) 131–133, 150
 - ... capability 65, 132–133, 151
 - ... discretionary (D-AC) 144, 151
 - ... mandatory (M-AC) 144–145, 152
 - ... ticket (capability) 132–133
- Access Control Entry (ACE) 130–132, 149
- access control indicator 128–129, 133, 149
- Access Control List (ACL) 131–134, 136, 149, 151
- access control matrix 130–132, 149, 151–152
- access matrix, *see*: access control matrix
- account 56
- account recovery 13, 58, 64–65, 67, 73, 262
- accountability 3–4, 23, 129, 133, 234
- ACK flag 284–285, 304
- ACK storm 331
- acknowledgement number (TCP) 305, 329–330
- ACME (certificate management) 230, 270
- active attack, *see*: attack
- active content 185, 200, 246, 248, 259–260, 286
- ActiveX controls 200, 259
- address bar, *see*: URL bar
- address resolution attacks 185, 204, 325–329
- Address Resolution Protocol (ARP) 303, 327, 334
- Address Space Layout Randomization (ASLR) 170, 173–174, 179
- address spoofing, *see*: IP address (spoofing)
- Administrator (Windows) 156
- Adobe Flash 194, 200, 259
- Adobe PDF 189
- Adobe Reader 259
- Advanced Encryption Standard (AES) 21, 33–34, 48–51, 203, 254, 274
- adversary (opponent) 5, 25
- adversary classes, *see*: adversary model
- adversary model 8–11, 19, 27, 320, 340
 - ... attributes 9–10, 19
 - ... capability-level schema 10
 - ... categorical schema 10
 - ... named groups 10, 19
- advertising model (Internet) 257
- AEAD (Authenticated Encryption with Associated Data), *see*: authenticated encryption
- AES, *see*: Advanced Encryption Standard
- Ajax (Asynchronous JavaScript and XML) 260, 275
- alarm (IDS) 310–315
- alarm imprecision 312–313
- alarm precision 312–313
- algorithm 30
- algorithm agility 24
- ALU, *see*: Arithmetic Logic Unit
- ALU flags 163–165, 178
- amplification (DoS) 322–325, 334
- anchor tag (HTML) 247
- Anderson report (1972) 152
- Anderson report (1980) 332
- Android (OS) 146
- Annual Loss Expectancy (ALE) 7
- anomaly-based IDS, *see*: IDS
- anonymity 4, 239
- anti-detection (malware) 191
- anti-virus 185, 190, 197, 313, 320
- ANX (Automotive Network eXchange) 224
- API hooking, *see*: hooking
- application-level filter, *see*: firewall
- Argon2 (hashing) 61, 86
- arguments (argv) 177
- Arithmetic Logic Unit (ALU) 163, 165
- ARM (ARMv7) 151, 178
- ARP, *see*: Address Resolution Protocol
- ARP cache 328
 - ... cache poisoning 328
- ARP spoofing (MAC address) 316, 325, 327–329, 331, 334
 - ... defenses 328
- ARP tables 328
- arpspoof 329
- ASCII character 34, 107, 203, 236, 265–266
- ASLR, *see*: Address Space Layout Randomization
- assembly language 163, 208
- asset 4
- assumptions 11, 16, 18, 24, 27, 71, 165, 340–341
- assurance 19–20
- asymmetric cryptography, *see*: public-key crypto
- atomic transactions 158
- attack (approaches, methods) 5, 27, 99
 - ... active vs. passive 32, 94, 102, 107, 254
 - ... breadth-first search 57, 84
 - ... brute-force 23, 61, 107
 - ... forward search 68, 99, 111–113
 - ... generic vs. targeted 8, 10, 57, 60, 66
 - ... interleaving 66, 98–99, 120
 - ... network-based 310, 320–332
 - ... pre-capture (pre-play) 68, 99
 - ... precomputation (hash function) 44
 - ... reflection 98–99
 - ... relay 98–99, 103, 269
 - ... replay 40, 67, 97, 99, 254, 302

- ... *see also*: Denial of Service, dictionary, exhaustive search, impersonation, middle-person, social engineering
 - attack libraries 27
 - attack models (biometrics) 87
 - attack models (ciphers) 32
 - ... chosen-ciphertext 32
 - ... chosen-plaintext 32
 - ... ciphertext-only 32
 - ... known-plaintext 32, 111
 - attack patterns 178
 - attack surface 20–21, 78, 238, 287, 319, 327
 - attack trees 13–14
 - attack vector 5, 13–14, 26, 320, 327
 - attacker 5, 195
 - ... active vs. passive 32, 102
 - attacks on password authentication 15, 57–58, 78
 - attribute (certificate) 215
 - attribution 4
 - audit log 23, 129, 133, 196, 250, 283, 287, 310–311, 315–316, 332
 - audit trail, *see*: audit log
 - AUTH TLS 254
 - authenticated encryption (AE) 36, 47–49, 51, 253–254, 274
 - ... CCM mode 47–49, 51, 274
 - ... GCM mode 49, 51, 274
 - ... generic composition 47–48
 - ... OCB mode 51
 - authenticated key establishment 92, 94, 105, 120, 253, 294
 - authenticated key exchange, *see*: authenticated key establishment
 - authentication 3, 56, 92, 214
 - ... *see also*: challenge-response, data origin authentication, entity authentication, user authentication
 - authentication cookie 260, 265
 - authentication factors (vs. signals) 70
 - Authentication Header (IPsec AH) 300–303, 305, 306
 - authentication protocol mistakes 97–99
 - authentication protocols 92–94, 97–100
 - authentication signals (vs. factors) 70
 - authentication token (authenticator) 65, 69, 113
 - authentication tree, *see*: Merkle tree
 - authentication-only protocols 93, 112
 - authenticator, *see*: authentication token
 - authenticity 214
 - Authenticode (code signing) 208
 - authoritative DNS name server 326–327
 - authorization 3, 56, 214
 - auto-rooter (malware) 192, 319
 - Automated Turing Test (ATT) 80
 - availability 3, 320
- ## B
- Babylonia virus (dropper) 202
 - backdoor (malware) 192, 195–196, 202, 207, 320
 - backscatter 321, 334
 - backup 37, 43, 57, 94–95, 185, 202
 - Balloon (hashing) 86
 - BAN logic 105, 120
 - barn door problem 273
 - base and bounds registers 127–129
 - Base Pointer (BP), *see*: Frame Pointer
 - base rate fallacy 313–313, 333
 - base rate of incidence (IDS) 312–313
 - bash (shell) 171
 - basic constraints (extension) 221
 - bastion host 291–292
 - Bayesian detection rate 313
 - bcrypt (hashing) 61
 - bearer token 132
 - behavioral authentication 71
 - Berkeley r-commands (r-utilities) 194, 293
 - /bin/login, *see*: login
 - /bin/sh 171
 - binary (file), *see*: object (file)
 - binary analysis 164, 173
 - binary entropy function 83
 - biometric authentication 45, 69, 71–76, 86–87, 311–312
 - ... behavioral biometrics 71–72, 87
 - ... circumvention 76
 - ... disadvantages 72
 - ... evaluation of 75
 - ... physical biometrics 71–72
 - ... usability 73, 75
 - biometric modalities 71–72, 76
 - biometric template 45, 56, 72–74
 - BIOS (basic input/output system) 188–189
 - birthday paradox 43–44
 - bitcoin (Bitcoin) 44, 202, 206
 - black-box vs. white-box 10–11, 34
 - black-hat vs. white-hat 178–179, 316–318, 320
 - blacklist vs. whitelist 21, 43, 63–64, 85–86, 190, 251, 265, 268–269, 271, 285, 287, 314, 318, 325, 333
 - blind TCP reset 332
 - block cipher 34
 - block cipher algorithms, *see*: AES, DES, triple-DES
 - blocklength 34
 - Blue Pill (rootkit) 208
 - boot process (boot loader) 199
 - boot sector 188–189, 204
 - bootkit 188
 - bot (robot) 79, 203, 322–323
 - botnet 192, 196, 202–203, 208, 321, 323, 325
 - ... and crime 203
 - ... herder (botmaster) 203–204, 321

- ... incidents 204
 - ... motivation 204
 - botnet communication structure 203
 - bounds checking 173, 179
 - bracket (RWX), *see*: protection rings
 - Brain virus 188–189
 - bridge CA trust model 224–226, 228, 241
 - Bro, *see*: Zeek
 - broadcast (address, message) 323, 328
 - browser
 - ... chrome (border) 270
 - ... extensions 260
 - ... history 250
 - ... mobile browsers 275
 - ... plugins 259–260, 274
 - ... proxy settings 251
 - ... session 255, 260
 - ... trust model issues 232–233
 - browser products
 - ... Chrome (Google) 219, 231, 257, 271–272, 275
 - ... Firefox (Mozilla) 232–233, 271
 - ... Internet Explorer (Microsoft) 259
 - ... Safari (Apple) 271
 - browser security 246–275
 - browser trust model 227, 229–234, 272, 274, 294
 - brute force, *see*: attack
 - BSD packet filter (BPF) 319, 333
 - BSS (Block Started by Symbol) 166–167
 - bucket brigade attack, *see*: grandmaster postal chess
 - buffer overflow attack 156, 163, 166–167, 179, 333
 - ... defenses 172–174, 179
 - buffer overrun, *see*: buffer overflow
 - bump in the stack (IPsec) 303
 - bump in the wire (IPsec) 303
- ## C
- C language 178
 - C language vulnerabilities 159–166, 178
 - C# 173
 - C++ 160, 164
 - CA, *see*: Certification Authority
 - CA compromise incidents 232
 - CA Revocation List (CARL) 223
 - CA-certificate 221, 225, 229
 - CA/browser forum 230, 241
 - caching (HTTP) 250
 - Caesar cipher 31
 - canary (heap) 173, 179
 - canary (stack) 172–173, 179
 - canonical representation 23, 265
 - ... *see also*: traffic normalization
 - capability 65, 132–133, 151
 - CAPEC (Common Attack Pattern Enumeration and Classification) 27
 - CAPTCHA 66, 79–81, 87
 - CARL, *see*: CA Revocation List
 - carry flag (ALU) 164–166, 178
 - casting, *see*: type casting
 - cat and mouse 190, 269
 - CBC (Cipher Block Chaining), *see*: modes of operation
 - CBC-MAC, *see*: MAC algorithms
 - CCured 179
 - CDN, *see*: Content Delivery Network
 - centralized symmetric-key servers, *see*: KDC, KTC
 - certificate (public key) 49, 214–215
 - ... browser interface (TLS) 232
 - ... chain 24, 217–218, 221, 223, 226, 231–234, 237, 271–272, 274
 - ... chain length 221
 - ... chain validation 217–218, 223
 - ... closed system 224–225, 238–239
 - ... code signing 185, 208, 221
 - ... cross-certificate (pair) 221, 225–228
 - ... disadvantages 237
 - ... extension fields (X.509v3) 215, 220–221, 228, 230, 241
 - ... grades (classes) 229–230
 - ... key usage 221
 - ... policy constraints 218, 221, 228
 - ... pros and cons 237–238
 - ... request 24, 216
 - ... reverse 226, 228
 - ... self-signed 218–219, 230–232
 - ... short-lived 222–223
 - ... substitution attack 233
 - ... TLS certificate 229–234
 - ... untrusted (accepting) 219
 - ... validation 217–218, 237, 272
 - ... X.509 215, 217, 238–239, 241
 - certificate directory 216–217, 229, 237–239
 - Certificate Management Protocol (CMP) 216, 241
 - Certificate Practice Statement (CPS) 230
 - certificate profile 217, 241
 - certificate revocation 49, 221–224, 230, 233, 237–238, 240–241
 - ... approaches 222–223
 - ... reasons 221–222
 - ... revocation list (CRL) 222, 239
 - ... timeline 222–223, 241
 - ... revocation tree (CRT) 241
 - Certificate Transparency (CT) 234
 - certificate trust models 224–229, 241, 294
 - Certification Authority (CA) 49, 215–217
 - certification policy, *see*: policy
 - certification request 24, 216–217
 - CFB (Cipher Feedback Mode), *see*: modes of operation
 - CGI script 264
 - ChaCha20 (stream cipher) 47–49, 51, 254, 274
 - challenge ACKs (TCP) 334

- challenge questions 65–66
- challenge-response 49, 69, 97–100, 112, 216
- channel security (TLS, HTTPS) 271, 274
- char data type (C) 160
- character encoding 265–266, 268–269
- character string (C), *see*: string
- check on first use (COFU) 220
- checksum 3, 41, 111, 305
- CHERI capabilities 151, 341
- Chernobyl virus (CIH) 189
- chgrp (command) 136
- child process (OS) 137, 171, 175–177
- chmod (command) 136
- chokepoint 21, 285
- chosen-ciphertext attack, *see*: attack models (ciphers)
- chosen-plaintext attack, *see*: attack models (ciphers)
- chown (command) 136
- chrome, *see*: browser (chrome)
- chroot (system call) 142, 151, 333
- chroot jail, *see*: jail
- cipher 32–34
 - ... classical 51
 - ... common 49
- ciphertext 31
- ciphertext-only attack, *see*: attack models (ciphers)
- circuit-level proxy, *see*: firewall (proxy)
- claimant 92–93
- clandestine user 332
- Clang (compiler) 164
- classification level (clearance) 144
- classification of attackers, *see*: adversary model
- clearance, *see*: classification level
- cleartext, *see*: plaintext
- clone (OS process) 176–177
- cmd.exe (Windows) 177
- CMP, *see*: Certificate Management Protocol
- CMS, *see*: Cryptographic Message Syntax
- code inspection (manual) 11, 179
- code point, *see*: character encoding
- Code Red (worm) 208
- Code Red II (worm) 192
- code signing 185, 208, 221
- cognitive walkthrough (usability) 340
- collision (hashing) 42, 44, 51
- collision resistant 42–43
- combining encryption and MAC, *see*: order of combining signing and encrypting, *see*: order of
- command and control (botnet) 203–204, 325
- command line argument 167, 169
- command line interpreter, *see*: shell
- command shell, *see*: shell
- community of trust 113, 221–222, 225–229, 238–240
- compatibility 25, 78, 86, 150, 172, 174, 235, 238, 265, 269
- compelled certificate attack 234, 241
- compiler 196–197, 199
- complete mediation, *see*: design principles
- complete network 225
- computational security 33, 42
- computer security 2, 5, 18
- Concept virus 189
- conditional probabilities 313
- confidentiality 3–4, 229
- Conficker (worm botnet) 208
- configuration errors 317
- confinement problem 152
- confounder 99, 112
- confused deputy 200, 262
- congruence (modular arithmetic) 38–39, 50, 115–119, 252
- CONNECT (HTTP request method), *see*: HTTP CONNECT
- connection forwarding 293
- connection-oriented 304
- connectionless 304
- connectivity 25
- content body (email message) 235–236
- Content Delivery Network (CDN) 234, 241, 254, 325, 334
- content header (email message) 235–236
- content inspection 286, 290–291, 299
- content scanning (email) 238, 240
- content scanning (HTTPS) 254
- Content Security Policy 265, 275
- contextualized signatures (IDS) 333
- control flow (integrity) 161, 169–170, 173–174, 179, 208, 315
- cookie (HTTP), *see*: HTTP cookie
- Cookie (HTTP header) 255
- COPS (scanner) 319, 333
- CORS (Cross-Origin Resource Sharing) 275
- cost-benefit analysis 8, 174
- Counter mode with CBC-MAC (CCM), *see*: authenticated encryption
- countermeasure 6
- covert channel 29, 152
- cp (copy) 293
- CRC (Cyclic Redundancy Code) 42
- credential 100, 113, 264, 271
- credential manager 113
- credentialed scanning 317, 333
- CRL, *see*: certificate revocation (revocation list)
- CRL distribution point 222
- CRL fragments 222
- cross-certificate pair, *see*: certificate
- cross-check 24, 173, 198, 218, 220, 230, 232, 239, 294
- cross-frame communications 274
- cross-origin communications 274
- cross-site request forgery (CSRF) 260–262, 264, 275
 - ... defenses 262, 265

- cross-site scripting (XSS) 262–266, 274–275
 - ... defenses 264–265, 275
 - cross-view difference (rootkit detection) 200
 - cruiseline certificate 234
 - crypto-strength key vs. weak secret 95
 - cryptographic key, *see*: key
 - Cryptographic Message Syntax (CMS) 241
 - cryptographic protocol 92, 120, 214
 - cryptography 30, 51, 214
 - cryptosystem 31
 - cryptovirology 208
 - CSRF, *see*: cross-site request forgery
 - CTR (counter mode), *see*: modes of operation
 - cued recall 65, 79
 - cumulative probability of success 85
 - CVE list (Common Vulnerabilities and Exposures) 208, 319
 - CVSS (Common Vulnerability Scoring System) 208
 - CWE dictionary (Common Weakness Enumeration) 208
 - cyclic group 115–120
 - Cyclic Redundancy Code, *see*: CRC
 - Cyclone (C dialect) 179
- ## D
- daemon (service) 175, 304, 318
 - DANE certificate 234
 - DANE protocol 234
 - dangerous error 273
 - dangling pointer 179
 - darknet 206
 - Data Encryption Standard, *see*: DES
 - data execution prevention (DEP), *see*: non-executable
 - data extrusion 283
 - data flow diagram 12, 14
 - data integrity, *see*: integrity
 - data link (OSI layer 2) 300, 328
 - data origin authentication 3, 39, 45–47, 253
 - data remanence, *see*: secure deletion
 - data segment (OS) 167–168
 - data-type verification, *see*: design principles
 - datablock (filesystem) 138, 140, 142, 157
 - datagram 300, 302–305
 - DDoS, *see*: Distributed Denial of Service
 - DDoS toolkits 325
 - debug (command) 194
 - decentralized CA trust 227–228
 - deceptive URL (look-alike) 270
 - decryption 30–31
 - ... *see also*: block cipher, public key, RSA, stream cipher
 - deep packet inspection 287
 - default deny (rulesets) 284–285
 - ... *see also*: design principles (safe defaults)
 - defense in depth 286–287
 - ... *see also*: design principles
 - deleting (files, data) 23, 104, 143–144
 - ... *see also*: secure deletion
 - delta CRL 222
 - demonstration of knowledge, *see*: proof of knowledge
 - Denial of Service (DoS) 3, 6, 15, 24, 187, 193, 284, 320–325, 328, 333–334
 - ... defenses 325
 - ... motives 320
 - ... on revocation 223–224
 - dependability 27
 - dependable and secure computing 27, 184
 - DES (block cipher) 32, 49, 51
 - descriptor register 127–128, 149
 - descriptor segment 128–129, 149–150
 - design for evolution, *see*: design principles
 - design principles for security 20–25, 27, 151, 206, 273
 - ... complete mediation (P4) 21, 25, 131, 134, 146, 157, 234, 283, 324
 - ... data-type verification (P15) 23, 25, 165, 173, 265, 333
 - ... defense in depth (P13) 23, 50, 64, 66, 70, 73, 78, 233, 291
 - ... design for evolution (HP2) 24, 60
 - ... evidence production (P14) 23, 234, 311, 316
 - ... independent confirmation (P18) 24, 25, 70
 - ... isolated compartments (P5) 21–22, 128, 142, 146, 197, 199, 206, 257, 283, 297, 324
 - ... least privilege (P6) 21–22, 129, 137, 148, 151, 174, 199, 206, 234, 291, 297, 324
 - ... least surprise (P10) 22, 206, 273
 - ... modular design (P7) 21–22, 131, 146, 151, 199
 - ... open design (P3) 21, 24, 31, 41, 80
 - ... reluctant allocation (P20) 24, 262, 323–324
 - ... remnant removal (P16) 23, 104, 144
 - ... request-response integrity (P19) 21, 24, 158, 218, 325, 328
 - ... safe defaults (P2) 20–21, 206, 224, 233–234, 273, 284
 - ... security by design (HP1) 24
 - ... simplicity and necessity (P1) 20, 26, 78, 206, 324
 - ... small trusted bases (P8) 22, 131, 152
 - ... sufficient work factor (P12) 23, 32, 64, 70, 111
 - ... time-tested tools (P9) 22, 30, 97, 106
 - ... trust anchor justification (P17) 23–25, 218, 220, 234
 - ... user buy-in (P11) 23, 58, 75, 273
 - desynchronization (TCP session) 331
 - DET, *see*: Detection Error Tradeoff
 - detached signatures (S/MIME) 238
 - Detection Error Tradeoff (DET) 74–75
 - detection rate (true positive rate) 312
 - detection vs. prevention 19, 23, 311
 - detour patching 198

- device fingerprinting 70, 80
 - device pairing methods 120
 - DH, *see*: Diffie-Hellman
 - DHCP (Dynamic Host Configuration Protocol) 327
 - dictionary attack 57, 60, 63–64, 86, 92, 97–99, 107–111
 - Diffie-Hellman (DH) key agreement 38, 50–51, 93–94, 100–103, 109–110, 115–121, 236, 252, 274, 300, 306, 323
 - ... ephemeral (DHE) 252–253
 - ... parameter checks 118–119
 - digital evidence, *see*: evidence
 - digital signature 39–41, 44, 216
 - ... comparison to public-key encryption 40
 - ... generation and verification 40
 - ... using hash function 44–45
 - ... with appendix 51
 - ... with message recovery 51
 - digital signature algorithms, *see*: RSA, DSA, ECDSA, EdDSA
 - directory, *see*: certificate directory
 - directory permissions, *see*: permissions
 - directory structure 138, 140, 142, 151
 - dirfile (directory file) 138
 - discrete logarithm 50, 101, 117, 121
 - disk encryption 200, 208
 - dispatch table 169, 197–198
 - distance-bounding protocols 38
 - distinguished name (DN) 215
 - Distributed Denial of Service (DDoS) 203, 207, 234, 321, 325, 333
 - diversity of code 22
 - DKOM (direct kernel object manipulation) 198
 - DLL (Dynamically Linked Library) 198–199
 - DLL injection (interception) 200, 208
 - DMA (Direct Memory Access) 199
 - DMZ (demilitarized zone) 285, 291–292
 - DN, *see*: distinguished name
 - DNS (Domain Name System) 235, 246–247, 282, 284–285, 291–292, 300, 304, 306, 325, 334
 - ... attacks on (by domain exploited) 327
 - ... cache poisoning, *see*: DNS (spoofing)
 - ... client cache 326–327
 - ... global hierarchy 326
 - ... lookup 326
 - ... records 229, 234
 - ... resolution 204, 247, 326–328
 - ... resolver 326
 - ... resolver cache 326–327
 - ... root 247
 - ... root server 326
 - ... server 326–327
 - ... server settings 327
 - ... spoofing 327
 - ... threat analysis 334
 - DNS security, *see*: DNSSEC
 - DNSSEC (DNS security extensions) 234, 327, 334
 - document object (HTML), *see*: DOM
 - document.cookie 256, 263, 265
 - document.domain 255, 259
 - document.getElementById 263
 - document loading (HTML) 248
 - document.location 255, 263
 - document.URL 255
 - document.write 248, 265
 - DOM (Document Object Model) 255, 274
 - DOM-based XSS 263
 - domain, *see*: protection domain
 - Domain (cookie attribute) 255–256, 259
 - domain blacklisting 271
 - domain mismatch error 232
 - domain name (DNS) 247
 - Domain Validated (DV certificate) 229, 231, 270–272
 - DoS, *see*: Denial of Service
 - double-free (memory management) 179
 - downloader, *see*: dropper
 - downloader graph 201, 208
 - drive-by download 170, 185, 200–201, 207–208, 252, 265, 286
 - dropper (malware) 201–202, 208
 - DSA (Digital Signature Algorithm) 51, 121, 274
 - DSA prime 117–119, 121
 - DSA subgroup 118–119
 - dsniff (sniffing toolset) 328–329
 - dual-homed host 287, 289, 291
 - DV, *see*: Domain Validated
 - dynamic analysis 173
 - dynamic linker, *see*: linking and loading
 - dynamic memory allocation 169
 - dynamic packet filter 284, 286–287, 306
- ## E
- Easter egg (software) 205
 - eavesdropping 18, 31, 67, 94, 101–102, 196, 238, 297
 - ECB (Electronic Codebook Mode), *see*: modes of operation
 - ECDSA, *see*: elliptic curve Digital Signature Algorithm
 - echo request (echo reply), *see*: ping
 - EdDSA, *see*: Edwards-curve DSA
 - education (training) 25–26, 79, 185, 269, 271, 273
 - Edwards-curve DSA (EdDSA) 253
 - effective key space, *see*: key space
 - effective UID (eUID), *see*: UID
 - egress filtering 284–285, 323–325
 - EKE, *see*: Encrypted Key Exchange
 - elevation of privilege, *see*: privilege escalation
 - ElGamal encryption 101
 - ElGamal key agreement 101

- elliptic curve cryptography (ECC) 50–51, 252–253
 - elliptic curve Diffie-Hellman Ephemeral (ECDHE) 252
 - elliptic curve Digital Signature Algorithm (ECDSA) 51, 253
 - email
 - ... forwarding 238
 - ... lists 238
 - ... tracking 257
 - ... transfer model 235
 - ... virus (email worm) 187, 189, 191, 238
 - ... worm-virus incidents 191
 - email encryption 38, 235–240, 254, 275
 - ... body 235
 - ... email filtering 291
 - ... header 235
 - ... link-by-link 254
 - ... measurement studies 254
 - ... message key 236
 - ... message structure 235–236
 - ... security header 236
 - ... status in practice 240
 - embed tag (HTML) 259, 265
 - emulator (emulation tools) 190–192
 - Encapsulating Security Payload (IPsec ESP) 300–306
 - encapsulation 288, 298, 300, 302
 - encrypted filesystem 200
 - Encrypted Key Exchange (EKE) 94, 107–110, 120
 - encryption 30–39
 - encryption (in RAM) 200
 - Enigma machine 51
 - enterprise PKI model 227–228, 239
 - enterprise SSO 113–114
 - entity 4, 15, 92, 104
 - entity authentication 3, 92–93, 100, 104
 - entity encoding 265–266
 - entropy 81–87
 - envelope (email) 235–236
 - envelope method of hashing, *see*: secret envelope
 - environment settings (envp) 177, 188
 - environment variables 167, 169
 - ephemeral 93, 104, 109, 120, 252–253
 - equal error rate (EER) 74–75
 - equivalent-strength keylengths 50
 - error rate example (IDS) 312
 - escalation, *see*: privilege escalation
 - escape (character, sequence) 265–266, 268–269
 - /etc/group 134
 - /etc/hosts.equiv 194, 297
 - /etc/passwd 57, 60, 134, 157–158, 194, 267
 - /etc/shadow 134
 - Ethereal, *see*: Wireshark
 - Ethernet 300, 304, 316–317, 327–328
 - ethical hacking 156
 - ... *see also*: responsible disclosure
 - Ettercap 328–329, 331, 334
 - Euler phi function (ϕ), *see*: phi function
 - EV, *see*: Extended Validation
 - EV guidelines 230, 241
 - evasive encoding (HTTP, HTML) 265–266
 - event 7, 82, 310–313, 315
 - event (browser) 248
 - event handler (browser) 248–249, 262
 - event outcomes (IDS) 311–312
 - event space 82
 - evidence 3, 311
 - evidence production, *see*: design principles
 - exclusive-OR, *see*: XOR
 - exec (system call) 137–138, 171, 176–177
 - execl (system call), *see*: exec
 - executable content, *see*: active content
 - execute bracket 148
 - execute permission (X), *see*: permissions
 - execve (system call), *see*: exec
 - exfiltration 283, 299
 - exhaustive search 31–32, 34, 50, 107
 - exit (system call) 172
 - expected loss, *see*: Annual Loss Expectancy
 - expected value 82
 - Expires (cookie attribute) 256
 - explicit key authentication 104–105
 - exploitation toolkits 317–318, 320, 333
 - exponent arithmetic 117, 119
 - export controls (crypto) 239
 - exposure maps 333
 - Extended Validation (EV certificate) 230–231, 241, 270–272
 - extension field, *see*: certificate (extension fields)
 - external penetrator 332
 - extrusion detection 333
- ## F
- facial recognition, *see*: biometric modalities
 - fail closed vs. fail open 21, 224, 233–234
 - fail-safe 21
 - failure to capture (failure to acquire) 72
 - failure to enroll 72
 - failures 27
 - fallback authentication 13, 72
 - false accept 73–74
 - false alarm (IDS) 173, 312, 314
 - false negative 311–313, 315
 - false negative rate (FNR) 312–313
 - false positive (FP, false alarm) 311–315, 317, 333
 - false positive rate (FPR) 312–313, 315
 - false reject 73–74
 - fault tree analysis 27
 - faults 27
 - favicon 271
 - federated identity system 113–114, 120

- feedback to user 273
 - FIDO (authentication) 86
 - file (filesystem) 126, 128, 138
 - file ACL 136
 - file allocation table (FAT) 189
 - file descriptor 158, 177, 304
 - file locker (malware) 202–203
 - file meta-data, *see*: inode
 - file squatting attack 159
 - file-based access control 133–134
 - filename resolution, *see*: name resolution
 - filepath, *see*: path
 - filesystem permissions 133–142
 - filter evasion, *see*: evasive encoding
 - filtering bridge 317, 333
 - FIN flag (TCP) 304
 - find (command) 139–140
 - finger (command) 193, 333
 - fingerd (daemon) 193
 - fingerprint, *see*: hash value
 - fingerprint cross-check 218, 220, 232, 241, 294
 - fingerprint recognition, *see*: biometric modalities
 - finite-field cryptography (FFC) 50, 252
 - firewall 192, 250, 282–292, 306, 311, 320, 325
 - ... application-level filter 287–291, 299, 306
 - ... architecture 12, 288–292, 306
 - ... configuration 306
 - ... dedicated 287
 - ... distributed 287, 306
 - ... internal 291
 - ... limitations 286
 - ... packet filter 282–288, 306
 - ... personal (host-based) 287–288
 - ... proxy (circuit-level) 286–292, 306, 325
 - ... proxy historical context 306
 - ... web application firewall 306
 - flag bits (TCP) 304–305
 - Flask security architecture 145
 - Flash cookie 259
 - flash crowd 334
 - flooding attack 320–321, 323, 331, 333
 - forensic analysis 23, 129, 133, 200, 287, 311, 316, 333
 - Foreshadow (hardware side channel) 341
 - forest of hierarchical trees 227
 - fork (system call) 137, 158, 171, 176–177, 296
 - form (HTML), *see*: web form
 - form tag (HTML) 248
 - formal analysis methods 339
 - formal security evaluation 10–11, 27
 - formal security models 27
 - formal verification 120
 - format string vulnerabilities 171, 179
 - forward search attack, *see*: attack
 - forward secrecy 93, 104, 109, 120, 252
 - fragment (packet) 290, 304–306, 321
 - fragmentation attack 290, 333
 - frame (data, Ethernet) 300, 303–304, 316, 328
 - frame (iframe, HTML) 201, 255, 257–260, 274
 - Frame Pointer (FP) 167
 - freshness (property) 46, 69, 72, 97–99, 101, 104–109, 216, 294
 - FTP (File Transfer Protocol) 229, 250, 254, 258, 286–287, 291–293, 297, 300, 304, 306
 - FTP normal mode 286–287
 - ftps (FTP over TLS) 293, 297
 - frapv (GCC compiler option) 166
 - fully qualified domain name (FQDN) 247, 249, 258
 - function call sequence (C) 167
 - function hooking, *see*: hooking
 - function pointer 169–170
 - fuzz testing (fuzzing) 179, 333
 - fuzzy commitment 45
- ## G
- gait, *see*: biometric modalities
 - gate extension 147–148
 - gate list 147
 - gateway 250, 282–292, 297–299, 302, 311, 325
 - gcc (GCC) 158, 164, 166
 - generative attacks 87
 - generator (group) 115–116
 - geolocation 70–71, 87
 - GET (HTTP request method) 249–250, 261–263, 274
 - getfacl (command) 136
 - GID, *see*: groupid
 - GNU C library 179
 - GNU Privacy Guard (GPG) 239
 - goals of computer security 2–4, 24
 - good key 104, 120
 - grandmaster postal chess attack 98, 103, 120
 - graphical passwords 78–79, 87
 - Green Book (rainbow series) 86
 - group (cyclic), *see*: cyclic group
 - group (protection group) 130, 132, 134
 - group identity (group identifier), *see*: groupid
 - group permissions 136
 - groupid (GID, groupID) 134, 137
 - guess count 85–86
 - guess number 84
 - guessing, *see*: password guessing
 - guessing function (guesswork) 84–85
 - guessing index 84
- ## H
- hacker vs. cracker 10
 - hand geometry, *see*: biometric modalities
 - Happy99 (worm-virus) 205

- hard link 142–144, 157
 - hardening a system 291
 - hardware redundancy 234, 325
 - hardware rings 150–152, 199
 - hardware security 152, 185, 197, 341
 - ... module (HSM) 64, 200
 - hardware tokens 56, 67, 69, 86
 - harmful software 184
 - hash chain, *see*: Lamport hash chain
 - hash code, *see*: hash value
 - hash function 41–45, 51, 61
 - ... collision resistant 42–43
 - ... GPU hashing 61, 86
 - ... iterated 60, 64, 86
 - ... one-way 41–42, 69
 - ... second-preimage resistant 42
 - ... specialized for passwords 61
 - ... used for digital signature 44
 - hash value (hash) 24, 41, 232, 239, 241, 294
 - Hashcat, *see*: oclHashcat
 - hashing algorithms 44, 61
 - heap allocator, *see*: secure heap allocator
 - heap memory 166
 - heap meta-data 169, 173, 179
 - heap spraying 168–170, 179, 200
 - heap-based buffer overflow 168–170, 178
 - Heartbleed incident 234, 241
 - heuristic evaluation (usability) 340
 - hidden filename extensions 205
 - hidden form 262
 - hierarchy (strict CA) 225–226, 233
 - hierarchy (with reverse certificates) 226
 - hijacking 94, 197, 329
 - ... based on address resolution 325–329
 - ... function calls, *see*: hooking
 - ... HTTP session 260, 329
 - ... system calls, *see*: hooking
 - ... TCP session 329–332, 334
 - ... TCP session (mitigation) 332
 - HKDF (HMAC-based KDF) 274
 - HMAC, *see*: MAC algorithms
 - HoneyD 333
 - honeypot (IDS) 196, 333
 - hooking 189–190, 196–200
 - host 247
 - hostname 247, 258, 325–327
 - hosts file 326
 - hotel safebox 16
 - href attribute (HTML) 247–248, 263
 - HSTS, *see*: HTTPS strict transport security
 - .htdigest file 100
 - HTML (Hypertext Markup Language) 200, 246–248
 - ... document 246, 255
 - ... email 201, 205–206, 238, 261, 264
 - ... parsing 248, 264–265, 274–275
 - ... special characters 266
 - HTML form, *see*: web form
 - HTML5 260, 274
 - HTTP (Hypertext Transfer Protocol) 247, 249–251, 255–256, 258, 260, 274, 284–285, 288, 291, 304
 - ... basic access authentication 100
 - ... CONNECT 249–251, 274
 - ... digest authentication 100, 120
 - ... proxy (abuse) 251, 261, 274
 - ... proxy server 234, 249–251, 274, 285–286
 - ... request 249–250, 253, 255, 261–262, 265, 267
 - ... request header 249
 - ... request method 249, 251
 - ... response 249–250, 253–254, 267
 - ... response header 249
 - ... status line 249
 - HTTP cookie (browser) 255–257, 260, 274
 - ... attributes 256
 - ... injection 274
 - ... protection and pitfalls 261
 - ... same-origin policy 259
 - ... theft 260–263, 265, 329
 - ... third-party cookies 257
 - ... viewing cookies 257
 - HttpOnly (cookie attribute) 256, 259–260
 - HTTPS (HTTP over TLS/SSL) 229, 233–234, 241, 250, 252–254, 258, 261, 270–271, 273–274, 285, 304, 306
 - ... encryption vs. site identity 271–272, 275
 - ... interception, *see*: TLS (interception)
 - HTTPS everywhere 233
 - HTTPS strict transport security (HSTS) 241
 - HTTPS-PAKE 273–274
 - hub 316
 - hub-and-spoke model 96, 225
 - human factors 26–27, 339
 - human-in-the-loop, *see*: CAPTCHA, usability and security
 - hybrid appliance 287
 - hybrid authentication protocol 94
 - hybrid encryption 38, 203, 236
 - hyperlink 247–248, 270
- ## I
- IAT, *see*: Import Address Table
 - ICMP 283–285, 300, 304–306, 318–319
 - ... destination unreachable 283, 305, 323
 - ... flood 323, 325
 - ... related attacks 324–325
 - identification 56, 76
 - identify friend-or-foe (IFF) 98
 - identity 3
 - identity provider (IdP) 113
 - identity theft 269, 271
 - IDEA (IDS) 332

- IDS, *see*: intrusion detection system
- IDS metrics 312
- IETF (Internet Engineering Task Force) xvii
- IFF, *see*: identify friend-or-foe
- IKE (Internet Key Exchange) 300, 303, 306
- image (executable) 199
- image tag (HTML) 247
- IMAP (email retrieval) 235, 254, 304
- immutable field 300
- impersonation 15, 73, 76, 87, 98–99, 103–104
- implicit key authentication 104–105
- Import Address Table (IAT) 198
- in-band signaling 218
- inbound 283–292, 304, 333
- independent channel 24, 67, 95, 294
- independent confirmation, *see*: design principles
- index of coincidence 51
- indirect CRL 241
- Individual Validated (IV) certificate 230
- infection vector 207
- information 82
- information-theoretic security 33, 42, 81
- ingress filtering 284–285, 323–325, 334
- inheriting UID 137–138, 176
- initial keying material, *see*: keying material
- Initialization Vector (IV) 35, 49, 301
- injection 156, 168, 248
 - ... code injection 23, 170–173, 176, 179
 - ... command injection 23, 200, 275, 329
 - ... command injection (formal definition) 267, 275
 - ... cookie injection 274
 - ... DLL injection (call interception) 200, 208
 - ... script injection 262–263, 265–267
 - ... SQL injection 266–269, 275
 - ... *see also*: buffer overflow, CSRF, XSS
- inline device 287, 297, 303, 316–317
- inode (index node) 135, 138, 140–142, 157–158
- input filtering 265–266, 268
- input sanitization 23, 262–265, 268–269, 275
- insider/outsider 9–10, 22, 185, 207, 282–283, 286, 299, 327
- instant-messaging system 225
- instruction address register, *see*: Instruction Pointer
- Instruction Pointer 147, 167–168, 170, 172, 178
- instruction set randomization 179
- integer conversion 160
- integer data types (C) 160
- integer factorization 50
- integer overflow, *see*: integer vulnerabilities
- integer truncation (C) 161–163, 165
- integer underflow, *see*: integer vulnerabilities
- integer vulnerabilities 159–166, 178
 - ... categories 162–163
 - ... extension value change 162–163
 - ... intentional overflow 165
 - ... narrowing loss 162–163
 - ... overflow 161–164, 178
 - ... signedness mismatch 159–163
 - ... underflow 162–163
- integrity (data) 3, 24, 33, 35, 39, 43, 45, 47
 - ... file checker, *see*: Tripwire
 - ... mechanisms 47
 - ... of public key 37, 214
- Intel (x86, IA-32) 151, 166, 178
- intelligent packet filtering 283
- interface design, *see*: usability and security
- interference (password) 59
- interleaving attack, *see*: attack
- intermediate CA 217–218, 225–226, 231–232, 234, 239
- Internet of Things (IoT) 310, 325
- Internet worm (Morris worm) 25, 57, 193–194, 297
- interoperability 25, 240, 274
- intruder 208, 282, 286, 311, 314–315, 332
- intrusion (incident) 310–311
- intrusion detection 306, 310–311
- intrusion detection system (IDS) 185, 192, 282, 306, 310–316
 - ... anomaly-based 314–316, 332
 - ... detection rules 314
 - ... historical context 332
 - ... host-based (HIDS) 311, 315, 320, 332
 - ... in practice 333
 - ... methodological approaches 313–316
 - ... network-based (NIDS) 311, 315–316, 320, 332
 - ... network behavior and analysis system (NBA)
 - ... signature-based 314, 332–333
 - ... specification-based 314–315, 333
 - ... wireless-based 320
- intrusion prevention system (IPS) 311, 317–318
- IP (Internet Protocol) 292, 300, 303–306
 - ... datagram 305
 - ... header 301–302, 305
- IP address 247, 303, 328
 - ... destination address 305
 - ... IPv4 192–193, 303, 323
 - ... IPv6 192, 303
 - ... resolution, *see*: DNS (resolution)
 - ... source address 305
 - ... spoofing 284, 321–322, 324–325, 330, 333
- IP-in-IP tunnel 302
- IPRA (Internet PCA Registration Authority, PEM) 239
- IPsec 224, 298–303, 306
 - ... deployment options 302–303
 - ... deployment challenges 302–303
 - ... ESP configurations 303
 - ... header 302
 - ... policy 303
 - ... trailer 302
- iptables 288, 306
- IRC (Internet Relay Chat) 204

iris recognition, *see*: biometric modalities
ISAKMP, *see*: IKE
isolated compartments, *see*: design principles
isolation 21, 127, 142, 146, 197, 199, 234, 246, 257,
283, 286–287, 291, 298, 316
ISP (Internet service provider) 324–327
issuer (certificate) 215
iterated hashing, *see*: hash function
IV (certificate), *see*: Individual Validated
IV (crypto), *see*: Initialization Vector

J

J-PAKE 111, 120, 273–274
jail (filesystem) 142, 151, 175, 333
... *see also*: chroot
Java 160, 173, 194, 259–260
... applet 200, 260
... Virtual Machine (JVM) 260
JavaScript 170, 200, 205, 248–249, 251, 255–260,
263–265, 274
... execution within browser 248
... URL, *see*: javascript:
javascript: (HTML pseudo-protocol) 248
JFK (IKE alternative) 306
JohnTheRipper (password cracker) 64
JSON (JavaScript Object Notation) 275
JSONP 275
jump table 169

K

Kaminsky attack (DNS) 327
Kasiski method 51
KDC, *see*: key distribution center
Keccak (hashing) 44
Kerberos 94, 96, 99, 113–114, 120, 294
Kerckhoffs' principle 21
kernel
... CPU mode, *see*: supervisor
... functionality 199
... memory 176, 195, 197
... module installation 199
key 22, 30
... backup and archival 37, 217
... decryption 31
... escrow 238
... long-term vs. session key 38, 93–95, 104, 120,
253
... master key 252–253
... public-private key pair 37
... re-use 95
... recovery 217
... registration 95
... resumption 254

... session key properties 104
... size 34
... symmetric key 32, 93
... working key (TLS session key) 252
key agreement 93–94
... *see also*: DH, ElGamal, EKE, PAKE, SPEKE,
STS
key continuity management 220, 241
key derivation function (KDF) 61, 101, 106, 252,
274
key distribution 37
... *see also*: key establishment, public-key distribu-
tion
key distribution center (KDC) 96, 114, 237
key establishment 92–97
key management 21, 38, 51, 94, 214, 216, 240
key revocation, *see*: certificate revocation
key server, *see*: key distribution
key-share 253–254
key space 31–34, 50, 61–63, 66, 79, 81, 95, 106, 111
key transfer, *see*: key transport
key translation center (KTC) 96
key transport 93, 96, 100–101, 236
... *see also*: KDC, Kerberos, KTC
Key-Usage constraint (extension) 221
key-use confirmation 99, 104–105, 119, 253
keyed hash function, *see*: MAC
keying material 93, 95–97, 101, 104, 236, 252, 254
keyjacking 200
keylength 34
... recommended 50
keylogger (keystroke logger) 18, 57, 196, 203, 207,
274
keyring, *see*: PGP
keystream, *see*: stream cipher
keystroke dynamics 87
knowledge-based authentication, *see*: what you know
known-key security 104
known-plaintext attack, *see*: attack models (ciphers)
KTC, *see*: key translation center
Kuang decision tree 27

L

Lamport hash chain 42, 67–68, 86
LAN (Local Area Network) 303, 316, 327–328, 331,
334
LAND (DoS attack) 321, 334
Latin-1 (character encoding) 266
law enforcement 196, 240
LDAP (Lightweight Directory Access Protocol) 222,
229, 238, 254
leap-of-faith (trust), *see*: trust on first use
least common mechanism 22
least privilege, *see*: design principles

- least surprise, *see*: design principles
 - legacy issues 25, 49, 160, 173–174, 236, 269, 286, 295, 298
 - length-preserving 35
 - Let's Encrypt (certificate service) 230, 270
 - libc (C library) 171, 173, 176–177, 179
 - libpcap 319
 - libraries (shared) 167, 197, 199–200, 217, 234
 - lifecycle 12, 19, 24
 - ... of password-authenticated account 13
 - ... of PKI components 217
 - ... of software development 11
 - link (system call) 141–142, 158
 - linking and loading (linkers) 199
 - Linux 126, 288
 - ... kernel backdoor 196
 - ... kernel module signing 208
 - ... Linux capabilities 22, 175, 199
 - ... security module (LSM) 145–146
 - listing (directory), *see*: ls
 - literal content (HTML, SQL) 266, 268
 - liveness property 104
 - ln (command), *see*: link
 - load balancing 325–326
 - loadable kernel module (LKM) 199
 - loader, *see*: linking and loading
 - location (HTML, HTTP) 255
 - Location (HTTP header) 255
 - lock icon (browser) 230–232, 270–272, 274
 - log, *see*: audit log
 - logarithm, *see*: discrete logarithm
 - logic bomb (malware) 204
 - logic of authentication, *see*: BAN logic
 - logical channel (SSH) 293–294
 - login (command) 138, 196
 - long-term key, *see*: key
 - Lotus Notes 241
 - ls (list command) 138, 141
 - lvtres (keylogger rootkit) 196
- ## M
- M-AC, *see*: mandatory access control
 - MAC, *see*: message authentication code
 - MAC address, *see*: media access control
 - MAC algorithms
 - ... CBC-MAC 46–47
 - ... CMAC (AES-CMAC) 46, 48, 51
 - ... HMAC 46, 48, 51, 274
 - ... Poly1305 46–49, 51, 274
 - MAC flooding 328
 - MAC table (network switch) 328
 - MAC truncation 47
 - machine learning 315
 - MacOS 333
 - Macromedia Flash, *see*: Adobe Flash
 - MACs from hash functions 46
 - ... *see also*: HMAC
 - malformed packets 321, 325
 - malicious scripts, *see*: CSRF, SQL (injection), XSS
 - malloc 162–163, 170–171, 178
 - malware (malicious software) 184–186, 205–207
 - ... classification 205–207
 - ... incidents 207
 - ... properties 207
 - man-in-the-middle attack, *see*: middle-person
 - mandatory access control (M-AC) 144–146, 152
 - mangling rules 64
 - manual gateway 289
 - market for lemons 26–27
 - Martian packets 323–324
 - mashup 274
 - masking (permission bits) 135–136, 141
 - masquerador 332
 - mass-mailing worm-virus 187, 189
 - master boot record (MBR), *see*: boot sector
 - master key, *see*: key
 - matching score (classification) 73–74
 - mathematical proof 17–18, 340
 - Max-Age (cookie attribute) 256
 - MDA (mail delivery agent) 235
 - MD5 (hashing) 44, 51, 61–62, 274
 - Mebroot (rootkit) 204
 - media access control (MAC) address 303, 316, 327–328
 - Melissa (virus) 189
 - Meltdown (hardware side channel) 197, 341
 - memory descriptor 127–128
 - memory layout 166–167
 - memory protection 127–129, 197
 - memory safety 163, 165, 172, 179
 - mental model 22, 142, 246, 269–270, 273, 275, 289
 - Merkle authentication (hash) tree 45
 - mesh trust models (ring-mesh) 225–228
 - message authentication 3, 45–47
 - message authentication code (MAC) 45–48, 64, 254
 - message digest, *see*: hash value
 - message expansion 35
 - metamorphic virus, *see*: virus
 - Metasploit 317, 320, 333
 - Meterpreter (Metasploit) 320
 - metrics, *see*: security metrics
 - microkernel 22, 152
 - Microsoft Outlook (Express) 189, 205
 - Microsoft Silverlight 259
 - Microsoft Word 189, 291
 - middle-person 57, 99, 102–103, 109, 118–119, 200, 234, 251–252, 254, 261, 270, 274, 288, 294, 327–329, 331
 - ... *see also*: HTTP proxy, TLS interception
 - middlebox 254, 261, 298
 - min-entropy 83, 85

minimize-secrets principle 22
 Mirai (botnet) 325
 misfeasance 332
 misuse detection (IDS) 332
 mixed content 274
 mkdir (command) 141
 MLS, *see*: multi-level security
 mobile phone (authentication), *see*: two-factor, what you have
 mod (modular arithmetic), *see*: congruence
 mode bit, *see*: supervisor
 model checking 179
 model-reality gap 16–18, 440
 modes of operation (block cipher) 35–36
 ... CBC 35–36, 274
 ... CFB 36
 ... CTR 35–36, 47
 ... ECB 35–36
 ... OFB 36
 ... XTS 36
 modification detection code 43
 modular design, *see*: design principles
 modular exponentiation 38–39
 modulus 38–39, 50, 108–109, 117
 monitoring system 311, 315–317, 332–333
 monolithic (vs. modular design) 131, 199
 Morris worm, *see*: Internet worm
 mother's maiden name, *see*: secret questions
 mouse patterns, *see*: biometric modalities
 MSA (mail submission agent) 235
 MTA (mail transfer agent) 235
 MTU (maximum transmission unit) 304
 MUA (mail user agent) 235
 multi-level security (MLS) 144, 151–152
 Multics 126, 133, 146, 148–152, 341
 multiplicative group 115, 117
 mutation engine (malware) 191
 mutual authentication 93–94, 100, 103, 106, 114, 223, 274

N

name (data type in certificate) 215
 name constraint (extension) 221, 228
 name resolution 24, 157–159, 178, 247
 name server (DNS) 326–327
 name space 113, 221, 239
 NAT (network address translation) 287, 303, 306
 National Vulnerability Database (NVD) 208
 navigator.cookieEnabled 256
 need-to-know (principle) 22
 Needham-Schroeder protocol 120
 Nessus (vulnerability scanner) 318–319
 Netcat (nc) 320
 Netfilter framework 288
 netstat (network statistics) 319

Network Flight Recorder (NFR) 332
 network interface card (NIC) 316
 network layer 291, 300, 303–305, 328
 network mapping 318
 network PKI 227
 network protocol stack 292, 298, 300, 303, 328
 network protocols 300, 303–306
 network security 282–306, 310–334
 network traffic analyzer 319
 network worm, *see*: worm
 Nimda (worm) 208
 NIST (National Inst. of Standards and Tech.) 34
 Nmap (network mapper) 318–319, 333
 NNTP (Network News Transfer Protocol) 254
 no-op sled (NOP, no-operation) 168, 170
 non-executable (stack, heap) 171–172
 non-repudiation 4, 15, 39, 45–46, 216–217
 nonce 35, 48–49, 99–100, 252–253
 notary 217
 NTAPI (Native API) 198
 NTP (Network Time Protocol) 324
 NUL byte (C) 167, 173, 177–178
 NULL pointer (C) 177
 null encryption (IPsec) 303
 NVD, *see*: National Vulnerability Database

O

obfuscation 191–192, 265, 268
 object (access control) 130–133, 145
 object (DOM), *see*: DOM
 object (file, binary) 199, 208
 object identifier (OID) 230
 object tag (HTML) 259, 265
 oclHashcat (password cracker) 64
 OCSP (Online Certificate Status Protocol) 222–223, 241
 OCSP-stapling 222
 OFB (Output Feedback Mode), *see*: modes of operation
 off-path (blind) attacks 332, 334
 offline password guessing 57–65, 77–78, 86, 92, 98, 105–111, 120, 217
 OID, *see*: object identifier
 OKE (Open Key Exchange) 111
 on-path attacks 329–331, 334
 onclick 248
 one's complement (binary representation) 164
 one-time pad (stream cipher) 33, 51
 one-time password (OTP) 17, 23, 67–70, 86, 99, 294, 329
 one-way hash function, *see*: hash function
 one-way property 41
 online password guessing 57–65, 78, 80, 84–86, 107–108, 120, 161, 306, 319

- online status checking (certificate) 222
 - onload 249, 262
 - onmouseover 248, 265
 - opcode (machine code) 168, 170, 177, 195, 199
 - open (system call) 157–159
 - open design, *see*: design principles
 - OpenID 120
 - OpenPGP 239, 241
 - OpenSSH 293
 - OpenSSL 22, 38, 232, 234
 - OpenVMS 151
 - OpenVPN 303
 - operating characteristic, *see*: ROC
 - operating system (OS) 151, 178
 - operating system security 126–152
 - operational practice (issuing certificates) 230, 241
 - opponent, *see*: adversary
 - opportunistic attacks 10
 - opportunistic encryption 21, 254
 - order (element, group) 115–116
 - order of encryption and MAC 40, 48
 - order of signing and encrypting 40, 238
 - orderly release (TCP) 304
 - Organization Validated (OV certificate) 230, 270, 272
 - origin (matching) 259
 - origin (SOP) 257–258
 - origin server 255–257, 260
 - origin triplet (SOP) 257–258
 - OS, *see*: operating system
 - OS fingerprinting, *see*: remote OS fingerprinting
 - OS/2 151
 - OSI stack, *see*: network protocol stack
 - OTP, *see*: one-time password
 - out-of-order execution (side channel) 197, 341
 - out-of-band (OOB) 95–96, 218–219, 237, 252, 306
 - ... *see also*: independent channel
 - outbound 283–292, 333
 - output escaping, *see*: escape
 - outsider, *see*: insider/outsider
 - OV, *see*: Organization Validated
 - overflow flag (ALU) 164–166, 178
 - OWASP 262, 269, 275
 - owner (file), *see*: user (file owner)
- P**
- p0f (OS fingerprinting) 318, 333
 - packet (networking) 303–306, 311
 - packet filter, *see*: firewall
 - packet-filtering rules 283–285, 306
 - packet sniffing (capture utilities) 316, 319, 332–333
 - padding 34, 301
 - padlock, *see*: lock icon
 - page reloads 260
 - paging (memory) 136
 - PAKE (password authenticated key exchange) 105–111, 120, 273–274
 - PAKE browser integration 273–274
 - parasite (hosted malware) 207
 - parent (OS process) 137–138, 158, 175–176
 - parser (HTML, JavaScript, URI, CSS) 275
 - ... *see also*: HTML (parsing)
 - partial-guessing metrics (passwords) 85–87
 - partitioned CRL 222
 - partitioning attack 108–109, 120
 - partitioning text 108
 - party, *see*: entity, principal
 - passcode generator 17, 68–70, 86
 - passive attacker, *see*: attacker
 - passkey (password-derived key) 64, 78, 295
 - passphrase 64, 69, 239, 295
 - passport analogy 218
 - passwd (command), *see*: /usr/bin/passwd
 - password 56–59, 129
 - ... advantages 59
 - ... attack defenses 60–65
 - ... capture 57–58
 - ... cracking tools 64
 - ... default 317
 - ... disadvantages 58
 - ... distribution (skewed) 63
 - ... length 62
 - ... master 77, 113
 - ... NIST guidelines 64–65, 87
 - ... pro-active checking 63
 - ... recovery, *see*: account recovery
 - ... stored hash 57
 - ... synchronization 77
 - ... system-assigned 61, 86
 - ... usability 58–59, 62, 64–65, 77, 339
 - ... user-chosen 63
 - ... verification using one-way function 43
 - password composition policy 5, 57–58, 63–65, 78, 87
 - password expiration policy (aging) 8, 13, 58, 62, 64–65, 86–87
 - password file, *see*: /etc/passwd
 - password generator, *see*: passcode generator
 - password guessing, *see*: online, offline
 - password guessing (SSH) 306
 - password hashing 43, 57
 - ... competition 61, 86
 - password managers 59, 76–78, 86–87, 113, 120, 275
 - ... derived passwords 77–78
 - ... password wallet 77–78
 - password meters 65, 87
 - password portfolios 87
 - password reset 65–66, 86
 - password sniffing, *see*: password (capture)
 - password stretching 60
 - password-authenticated key exchange, *see*: PAKE

- PasswordMultiplier 78
- patching (software update), *see*: update
- Path (cookie attribute) 256, 259
- path (pathname, filepath) 177, 247, 256, 258, 263
- path of least resistance 23
- path-access 139, 259
- path-based permissions, *see*: path-access
- pathLenConstraint (extension) 221, 228
- pathname resolution 143, 157–159, 178, 197
- PaX project (Linux) 179
- payload 38, 47, 187, 196, 283, 317
 - ... HTTP 251, 288
 - ... IPsec 301–302
 - ... TCP 304
- pay-per-install 208
- PBKDF2 (key derivation function) 61, 64
- PCA, *see*: Policy Certification Authority
- pcap 319
- PEM (Privacy Enhanced Mail) 235, 239, 241, 332
- pen testing, *see*: penetration testing
- penetration testing 10, 156, 179, 317–318, 320, 328, 333
- pepper (secret salt) 60, 64, 86
- percent encoding 266
- perfect forward secrecy, *see*: forward secrecy
- perimeter defense 17, 282–283, 285–287, 291, 318
 - ... *see also*: firewall
- Perl 264
- permission bits (filesystem) 128, 132
- permissions 128
 - ... on directories 138–139
 - ... on files 133
 - ... RWX 128, 132, 135–136, 138–139, 141, 148
- permutation 35, 193
- persistent cookie (HTTP) 255–256, 260, 262
- persistent state 259
- persona CA (PEM) 239
- personal knowledge questions, *see*: challenge questions
- PGP (Pretty Good Privacy) 220, 229, 235, 239–241, 275
 - ... key-packet 239–240
 - ... keyring 239–240
 - ... keyserver 240
 - ... lightweight certificate 239
 - ... signature packets 240
 - ... transferable key 240
 - ... trusted introducer 239–240
 - ... web of trust 228–229, 240
- PH-safe prime (Pohlig-Hellman safe) 117–119
- pharming 57, 185, 325–327
 - ... defenses 327
- phi function (ϕ) 38, 115
- phishing 17, 57, 77, 185, 206, 230, 238, 252, 264, 269–271, 275, 326, 339
 - ... and certificates 270
 - ... defenses 271
 - ... enablers 270, 275
- Photuris protocol 323
- PHP 264
- physical address (network) 303
- physical address space 199
- physical interface (switch port) 328
- PID, *see*: process identifier
- PIN (Personal Identification Number) 69–70, 72–73, 79, 95, 111–112
- ping (ICMP echo request) 284–285, 305–306, 321, 323
- Ping of Death (DoS attack) 321, 334
- ping sweep 306
- Pinkas-Sander login protocol 80–81, 87
- PKCS (Public Key Cryptography Standards) 216
- PKI (public-key infrastructure) 200, 214–217, 327
 - ... architectures 224–229, 241
 - ... components 216–217
 - ... lifecycle management 217
 - ... trust models, *see*: certificate trust models
- PKIX (PKI X.509-based standards) 241
- plaintext (cleartext) 31
- Pohlig-Hellman algorithm 117
- pointer arithmetic (C) 162, 165, 173
- pointer protection 173
- poison packets 321, 325, 331
- policy (security) 3–6, 18–19, 62, 282–284, 310, 318
 - ... access control 130–131
 - ... centrally defined 287
 - ... certificate-policies extension 230
 - ... certification policy 217–218, 230
 - ... compliance 317
 - ... corporate 294
 - ... cross-site access control 274
 - ... firewall 284–286, 288, 299
 - ... house policy 6
 - ... Internet (firewall) 284, 286
 - ... IPsec 303, 306
 - ... operational (CA) 216
 - ... policies for plugins 259
 - ... remote access policy 5
 - ... *see also*: password expiration, password composition
- Policy Certification Authority (PEM PCA) 239
- policy script component (IDS) 315
- policy-based packet filtering (IPsec) 303
- poly1305, *see*: MAC algorithms
- polyalphabetic substitution 51
- polymorphic virus, *see*: virus
- POP3 (email retrieval) 235, 254, 304
- port 175, 247, 258, 283–288, 295, 303–305, 318
- port forwarding (SSH) 295–296
- port mirror 316
- port scanning, *see*: scanning
- port stealing 328

- positive validation 269
 - POST (HTTP request method) 249, 261–262, 274
 - postMessage 274
 - postprocessing results (inline hooking) 198
 - pre-capture attack, *see*: attack
 - pre-shared key (PSK in TLS) 252–253
 - preimage 42
 - preimage resistance 41–42
 - prepared statements (SQL) 269
 - preview panes (email auto-preview) 205
 - primary group 134
 - primary vs. secondary task 273
 - principal 3, 21, 129–130
 - ... *see also*: subject (access control)
 - principles, *see*: design principles
 - printf (C function) 171
 - privacy 4, 75, 184, 250, 256–257
 - private key (asymmetric) 37–40, 45, 49–51, 101, 203, 214–217, 295–296
 - private network 298
 - private-key sharing (TLS) 234
 - private-key storage 214–215, 217
 - privilege escalation 16, 21, 156–157, 174–175, 178, 262
 - privilege level, *see*: protection rings, superuser, supervisor
 - privileged bit 127–128
 - ... *see also*: supervisor
 - privileged instructions 195
 - privileged port 175, 285
 - privileges 3, 22, 24, 129, 137, 150, 158, 174–175, 187, 195
 - proactive password cracking 317
 - probabilistic encryption, *see*: ElGamal encryption
 - probability distribution 74, 82, 85
 - probability of guessing success 62
 - probable prime number 333
 - probe (scan) 318, 333
 - process creation 175–176
 - process identifier (PID) 129, 137, 150, 319
 - processes (operating system) 149–151
 - profile (IDS) 314–315, 332
 - Program Counter (PC), *see*: Instruction Pointer
 - promiscuous mode (networking) 316, 319
 - proof by contradiction 190, 208
 - proof of knowledge 68, 97, 103, 112, 216, 229, 253
 - ... *see also*: challenge-response
 - protection 126
 - protection bit initial values 135, 141
 - protection domain 129–130, 149–151, 257
 - protection group, *see*: group
 - protection rings 146–152
 - protocol 92
 - protocol scrubber 333
 - provably secure 4
 - proxy (firewall), *see*: circuit-level proxy
 - proxy server, *see*: HTTP proxy
 - proxy-aware client 288–289
 - proxy-aware gateway 288
 - pseudo-protocol (HTML) 248
 - pseudo-random number generator (PRNG) 120
 - pseudonym 216
 - PSK, *see*: pre-shared key
 - psychological acceptability 273
 - public key pinning 241
 - public-key algorithms, *see*: Diffie-Hellman, ElGamal, elliptic curve, RSA
 - public-key certificate, *see*: certificate
 - public-key cryptography 32, 37–41, 51
 - ... encryption/decryption 37–39
 - ... signature/verification 39–41
 - ... symmetric vs. asymmetric 32, 37, 97
 - public-key distribution 37, 236–237
 - ... *see also*: Merkle tree
 - public-key infrastructure, *see*: PKI
 - public-key server 223, 237, 240
 - pull model, *see*: push
 - push vs. pull model 201, 222, 241
 - PuTTY (remote session utility) 297
 - PwdHash 78
 - Python 162
- ## Q
- query data (HTTP) 247, 250
- ## R
- RA, *see*: Registration Authority
 - rabbit (malware) 205, 321
 - race conditions (access control) 152, 157–159, 175, 178
 - ... *see also*: TOCTOU
 - rainbow tables 86, 107
 - random (number, key) 23, 33, 61, 79, 93, 95, 104, 108, 120, 159
 - random number (TVP) 93, 95, 97, 99, 112
 - random number generator (RNG) 95, 120
 - random variable 82
 - randomization of ephemeral ports 334
 - randomized encryption 101
 - ransomware 186, 196, 202–203, 206–208
 - ... incidents 203
 - rate limiting (throttling) 59, 63–64, 86, 161, 325
 - raw sockets 322
 - RC4, *see*: stream cipher
 - rcp (remote copy) 292–293, 296–297
 - read permission (R), *see*: permissions
 - reassembly (packet) 289–290, 304–306, 321, 333
 - receive window 302, 330–331
 - reconnaissance (scanning) 193, 316–320

- recursive query (DNS) 326
 - redirect CRL 241
 - redirection (HTTP response) 252
 - redirection (web) 200–201, 246, 251–252, 255, 263–265, 269
 - reduction modulo 2^n 162, 165
 - redundancy function 51
 - reference integrity, *see*: request-response integrity
 - reference monitor 130–132, 152
 - reference validation mechanism 131
 - REFERER header (HTTP) 249–250
 - reflected XSS (non-persistent) 263–264
 - reflection attack, *see*: attack
 - reflectors (networking, DoS) 333
 - Refresh header (HTTP response) 251
 - refresh meta-tag (HTML) 251
 - Registration Authority (RA) 217
 - regular expression 314
 - relational database 266
 - relative addressing 177–178, 188, 199
 - relay attack, *see*: attack
 - relocation 199
 - reluctant allocation 323
 - ... *see also*: design principles
 - relying party 49, 113, 215, 221–222, 224, 229, 236
 - remnant removal, *see*: design principles
 - Remote Access Trojan (RAT) 195
 - remote administration (remote desktop) 195
 - remote authentication 71–73, 214
 - remote desktop tools 195
 - remote OS fingerprinting 318, 333
 - remote shell 293
 - remote-access commands 292–293
 - replay attack, *see*: attack
 - replay protection (IPsec) 300–302
 - replay protection (TLS) 254
 - repository, *see*: certificate directory
 - resolve, *see*: DNS (resolution)
 - resource enumeration APIs 199
 - resource exhaustion 321, 325
 - responsible disclosure 317, 333
 - ... *see also*: ethical hacking
 - request URI (HTTP) 249–251, 256
 - request-response integrity, *see*: design principles
 - reset (TCP), *see*: RST
 - REST (Representational State Transfer services) 274
 - retinal scan, *see*: biometric modalities
 - return address 167–169, 171–173
 - return gate 148
 - return-to-libc 171–172, 179
 - reverse certificate 226
 - reverse engineering 185, 191–192, 204, 208
 - reverse Turing test, *see*: Automated Turing Test
 - revocation, *see*: certificate revocation
 - rexec (remote execution) 194, 292
 - RFC (IETF Request For Comments) 224
 - .rhosts file 296–297
 - Rijndael (AES) 34
 - ring (access control), *see*: protection rings
 - ... bracket 148
 - ... number 147, 150
 - ring-mesh, *see*: mesh trust models
 - risk 6, 78
 - ... assessment 6–9, 27
 - ... equation 6–7
 - ... management 9
 - ... rating matrix 9
 - RISOS report (1976) 152
 - rlogin (remote login) 194, 291–293, 297
 - ROC (receiver operator characteristic) 74–75, 87
 - rogue certificate 233, 241
 - role 129, 144–145
 - role-based access control (RBAC) 144–145, 151
 - root (UNIX) 134, 156
 - ... of filesystem 140
 - ... root privilege (UID 0) 134, 198
 - ... UID 0 vs. kernel 175
 - root CA 225–228
 - root of trust, *see*: trust anchor
 - root shell 175–176, 192
 - rooted (compromised) 195
 - rootkit (malware) 156, 189, 192–200, 204, 207–208
 - ... hypervisor 195, 208
 - ... postprocessing results (inline hooking) 198
 - ... Unix kernel rootkits 208
 - ... user vs. kernel rootkit 195, 197–200, 208
 - ... ways to install kernel rootkit 198–199
 - ... Windows kernel rootkits 208
 - ROP (return-oriented programming) 179
 - router 287, 291, 305, 332
 - ... *see also*: screening router
 - routing-based attacks 334
 - RSA 38–39, 41, 50–51, 69, 100, 108, 121, 203, 253, 274, 306
 - rsh (remote shell) 194, 292–293, 297
 - RST (TCP reset packet) 283, 304, 311, 322, 330–332
 - rule-based anomaly detection 332
- ## S
- S/KEY 86
 - S/MIME 220, 224, 235, 238–239, 241
 - SA, *see*: security association
 - safe boot 202
 - Safe Browsing project (Google) 271–272
 - safe C dialects 173, 179
 - safe C libraries 165, 173, 179
 - safe defaults, *see*: design principles
 - safe pathname resolution, *see*: pathname resolution
 - safe prime 110, 116–117

- salt (password) 60, 64, 112
- same-origin policy (SOP)
 - ... DOM SOP 246, 257–260, 274–275
 - ... SOP for cookies 259, 274–275
 - ... SOP for plugins 259, 274
- same-ports strategy 254, 274
- sandbox 21, 151, 174–175
- sanitization, *see*: input sanitization
- SATAN (audit tool) 319, 333
- saved UID (sUID), *see*: UID
- scan detection (IDS) 318, 333
- scanning 192, 318–320, 333
 - ... hit-list 193
 - ... Internet-scale 193
 - ... localized 192
 - ... permutation 193
 - ... stealthy 333
 - ... topologically aware 192–193
 - ... *see also*: reconnaissance
- scheme (retrieval scheme) 247, 258
- Schnorr signature scheme 121
- scp (secure copy) 293, 296–297
- screening router 287, 291–292, 320
- script tag (HTML) 248, 257, 263
- scripting languages 200, 248
- script (hash) 61
- SEAndroid (security-enhanced Android) 145–146
- search (command), *see*: find
- second-preimage resistant 42
- secret envelope (hashing) 46
- secret prefix (hashing) 46
- secret questions 65–66, 86
 - ... *see also*: account recovery
- secret suffix (hashing) 46
- secret validation tokens (CSRF) 262
- secret-key cryptography, *see*: symmetric cryptography
- secure 4–5, 18–20, 33
- Secure (cookie attribute) 256, 259, 261
- secure attention sequence, *see*: trusted path
- secure composition 340
- secure deletion 23, 104, 144
 - ... *see also*: remnant removal
- secure file transfer comparison 296–297
- secure heap allocator 171, 173, 179
- secure prime 118–119, 121
- secure protocol composition 341
- security analysis (process) 9–11, 17–19
- security association (IPsec SA) 300–301
- security by design, *see*: design principles
- security by obscurity 21
- security clearance, *see*: classification level
- security cues, *see*: security indicators
- security indicators (cues) 26, 246, 270–275, 339
 - ... negative indicators 272
- security kernel 131, 151–152
- security label 145
- security mechanisms 6, 18–19
- security metrics 27, 62, 75, 85–86, 312–313
- security model 11, 18, 260, 340
 - ... limitations 340
- Security Parameters Index (IPsec SPI) 300–301
- security policy, *see*: policy
- security policy database (IPsec) 303
- security questions, *see*: secret questions
- security requirements 5, 11, 18–20, 65, 75, 104, 126, 131, 340
- security tunnel, *see*: tunnel (encrypted)
- SecurityFocus vulnerability database 208
- segment (addressing) 128–129, 146–147
- segment (TCP) 300, 304, 329–331
- segment descriptor 128–129, 133, 146–150
- segmented addressing 126, 146, 152
- self-extracting executable 206
- self-replication (breeding malware) 207
- self-signed, *see*: certificate
- SELinux (security-enhanced Linux) 145, 151
- sendmail (program) 194
- sensor (IDS) 311
- separate-ports strategy 254, 274
- separation of duties 22
- sequence number
 - ... IPsec 300, 302
 - ... TCP 300–302, 305, 322, 324, 329–330
 - ... TVP 99
- sequences of system calls 311, 315
- server certificate, *see*: TLS certificate
- session creep (IDS) 315
- session hijacking, *see*: hijacking
- session ID (HTTP) 260, 294
- session key, *see*: key
- session resumption (TLS) 254
- session riding 261
- Set-Cookie (HTTP header) 255
- setfacl (command) 136
- setgid (set groupID) 135, 137–139
- setjmp/longjump 170
- setuid (set userID) 135, 137–139, 151, 157–158, 175
- sftp (SFTP) 293, 297
- SGX (Intel) 341
- SHA (Secure Hashing Algorithm) 44
- SHA-1 44, 61, 232, 274
- SHA-2 (SHA-256, SHA-512) 44, 232, 274
- SHA-3 44, 274
- shadow password file, *see*: /etc/shadow
- shadow stack 173
- Shannon entropy, *see*: entropy
- shell (command interpreter) 176–178, 188, 203, 293
- shell script 188
- shellcode 156, 170–172, 175–179, 203
- short exponents 50, 119
- shoulder surfing (password capture) 57

- side channels 15, 23, 197, 341
- sign bit 161, 164
- sign extension 161–163, 166
- sign flag (arithmetic) 166
- signed-only email 238
- signature (digital), *see*: digital signature
- signature (of attack)
 - ... behavioral 190, 314–315, 320
 - ... malware 190, 207, 314–315
- signature algorithm, *see*: digital signature algorithms
- signature verification, *see*: digital signature
- signature-based IDS, *see*: intrusion detection system
- signed code, *see*: code signing
- signed integer, *see*: two's complement
- signedness error (sign conversion), *see*: integer vulnerabilities
- SIM swap (attack) 67
- Simple Mail Transfer Protocol (SMTP) 229, 235, 254, 284–285, 304
- simplicity and necessity, *see*: design principles
- single-credential system 113
- single point of failure 23, 78, 204
- single sign-on (SSO) 113–114, 120
- single-CA trust models 224–225
- small trusted bases, *see*: design principles
- small-subgroup attack 101–102, 110, 118, 115–121
- SMS (Short Message Service) 66–67, 86–87, 240
- SMTP, *see*: Simple Mail Transfer Protocol
- Smurf attack (flood) 323, 325, 334
 - ... mitigation 323
- Snort 315, 319, 332–333
 - ... snort2bro 315
- social engineering 26, 57, 67, 185, 187, 199, 202, 205–207, 261, 264, 270–271, 273, 339
- sockd (SOCKS daemon) 289–290
- socket (IP) 284–285, 289–290, 304, 322, 330–331, 333
- SOCKS 289–290, 306
- software fault injection 333
- software installation 56, 185, 195, 205, 207
- software interrupt 164, 176
- software security 19, 156–178, 319
- Sony rootkit 196
- SOP, *see*: same-origin policy
- source address spoofing, *see*: IP address (spoofing)
- space (size of set), *see*: key space
- Spacefiller, *see*: Chernobyl virus
- spam 79, 203, 207, 238, 240, 271, 284–285, 291
 - ... filtering 240, 271
 - ... spambot 207
- SPAN port (switched port analyzer) 316–317
- spear phishing 270
- special protection bits 135–136
- specification-based IDS, *see*: intrusion detection system
- Spectre (hardware side channel) 341
- speculative execution (side channel) 197, 341
- SPEKE (Simple Password Exponential Key Exchange) 94, 110, 120
- SPI (IPsec Security Parameters Index) 300–301
- spoofing 15, 76
 - ... *see also*: ARP spoofing, DNS (spoofing), IP address (spoofing)
- SQL (Structured Query Language) 266
 - ... database 267
 - ... injection 266–269, 275
 - ... injection mitigation 269
 - ... query 267
 - ... server (database) 267
 - ... SQL single quotes 268
- squatting, *see*: typosquatting
- src= attribute (HTML) 247–248, 257
- SRP (PAKE protocol) 111, 120, 273–274
- SSDT (System Service Dispatch Table) 198
- SSH (secure shell protocol suite) 185, 220, 241, 250–251, 258, 290, 292–298, 300, 306
 - ... client authentication 294
 - ... connection protocol 293
 - ... host key 294, 306
 - ... host-based client authentication 296
 - ... multiplexed 293
 - ... server authentication 294
 - ... ssh, sshd (client, daemon) 293, 295
 - ... SSH tunnel 290, 292–293, 295–296, 300
 - ... SSH2 306
 - ... transport layer protocol 293
 - ... trust models 220, 294
 - ... user authentication protocol 293, 295
- SSL, *see*: TLS
- SSL history 241, 274
- Stacheldraht (TFN-based DoS) 325
- stack frame 167–168
- Stack Pointer (SP) 167
- stack querying 318, 333
- stack-based buffer overflow 166–168, 178, 193
- stakeholders 26, 240
- standard input/output streams, *see*: stdin
- startup file 139
- stat (system call) 159
- stateful packet filter 284
- stateful protocol analysis 332
 - ... *see also*: specification-based IDS
- stateless packet filter 284
- stateless protocol (HTTP) 255
- static analysis 173, 179, 269, 333
- statically allocated variables 167
- STARTTLS 254
- Station-to-Station (STS) key agreement 94, 103, 105, 120
- stdin (stdout, stderr) 175, 177, 293
- stealthy malware 189, 194, 207, 320, 333
 - ... *see also*: rootkit

- stepping stone 174, 206
 - sticky bit (filesystem) 135, 139, 158
 - store-and-forward 38, 104, 236–237, 288
 - stored XSS (persistent) 262–264
 - storing passwords, *see*: password file
 - strcpy (C library function) 167, 171–173
 - stream cipher 32–34, 36
 - ... RC4 49, 51, 274
 - ... stream vs. block cipher 36
 - ... Vernam cipher 32–34
 - ... *see also*: ChaCha20, one-time pad
 - STRIDE (threat modeling) 12, 15–16
 - string (NUL-terminated) 167, 173, 177, 179
 - strong password protocol, *see*: PAKE
 - strong prime 118, 120
 - strong secret, *see*: crypto-strength key
 - strongly typed, *see*: type safety
 - STS, *see*: Station-to-Station
 - Stuxnet (worm rootkit) 196
 - su (command) 137
 - subdomain (DNS) 247, 258–259, 270, 326
 - subgroup 115–116
 - subgroup confinement, *see*: small-subgroup attack
 - subject (access control) 130, 144–145, 149–151
 - Subject (certificate) 215, 221, 229–230, 232
 - Subject Alternate Name (SAN) 215–216, 218, 221, 232
 - subject-object model 130, 133, 149
 - submit button (web form) 249
 - subspace, *see*: space
 - SubVirt (rootkit) 208
 - sudo (command) 137
 - sufficient work factor, *see*: design principles
 - SUN 3 (workstation) 193
 - superuser (UID 0) 134, 140, 150, 174–176, 195, 199
 - supervisor (CPU mode) 127–128, 146, 149–151, 176, 195
 - supply chain 152, 185, 341
 - Suricata (NIDS) 332
 - surveillance 195–196, 206, 234
 - swapped memory 136, 199
 - switch 311, 316, 328
 - symbolic display (file permissions) 135–136
 - symbolic link (symlink) 142–144, 159
 - symmetric cryptography 22, 32–36, 41–49
 - symmetric key, *see*: key
 - symmetric-key algorithms 49
 - symmetric-key encryption 32–36
 - SYN cache 323
 - SYN cookies 323
 - SYN flood 321–323, 325, 334
 - ... mitigation 323, 334
 - SYN packet (flag) 304, 321–322, 329
 - SYN-ACK 284, 304–305, 322, 329–331
 - syscall, *see*: system call
 - syslog (utility) 283, 290, 306
 - system (syscall) 171–172
 - system call (syscall) 176–178, 185, 190, 197–198
 - system call hijacking, *see*: hooking
 - System Service Dispatch Table (SSDT), *see*: dispatch table
 - system specification 340
- ## T
- t-bit, *see*: sticky bit
 - taint analysis 269
 - tamper-proof 131
 - tampering (data integrity) 15
 - tap (test access port) 317
 - targeted attack, *see*: attack (generic vs. targeted)
 - TCP (Transmission Control Protocol) 229, 285, 289–290, 292, 297, 300, 303–306
 - ... amplification 324
 - ... connection 249, 290, 292, 295, 304, 329–330
 - ... connection set-up 304, 329–330
 - ... header 283, 304–305, 329
 - ... stream (relay of) 250–251
 - ... TCP session hijacking, *see*: hijacking
 - ... TCP/IP suite vulnerabilities 334
 - ... *see also*: three-way handshake
 - tcpdump (packet processing utility) 319
 - Teardrop (DoS attack) 321, 334
 - telnet (TELNET) 229, 291–293, 297, 329
 - temporary files 158–159
 - testing (security) 10–11, 19
 - ... functional vs. non-functional 11, 20, 340
 - ... *see also*: fuzz testing, penetration testing
 - TEtheral, *see*: Wireshark
 - text bit, *see*: sticky bit
 - text message, *see*: SMS
 - Thompson's Trojan compiler 152, 196–197
 - threat 5–6
 - threat agent 5
 - threat model 11–12, 16–19, 99, 274
 - ... browser 274
 - ... Internet 18, 27, 31
 - threat modeling 11–20, 27
 - ... DNS threat analysis 334
 - ... with architectural diagrams 12–13, 58
 - ... with checklists 12, 15
 - ... *see also*: attack trees, STRIDE
 - threat trees 27
 - ... *see also*: attack trees
 - three-way handshake (TCP) 304, 318, 322, 324, 329–331
 - threshold 22–23, 71, 73–74
 - throttling, *see*: rate limiting
 - ticket, *see*: access control (ticket)
 - ticket (Kerberos) 114, 294
 - time bomb (malware) 204
 - time-memory tradeoff 86, 107

- time-of-check time-of-use (TOCTOU) 157–159, 178
time-tested tools, *see*: design principles
time-variant parameter (TVP) 68, 99
... *see also*: nonce, random number, sequence number, timestamp
timestamp 99
timing attack (SSH) 306
TLD (top-level domain) 247
TLS (Transport Layer Security) 51, 229, 238, 241, 251–254, 273–274, 300
... certificate 218, 223, 229–234, 241, 253, 270–274
... certificate validation challenges (smartphones, non-browsers) 234–235
... channel 253
... encryption and integrity 253
... handshake layer 252
... history 241
... interception 251, 254
... key exchange 252
... layers 252
... master key 252
... record layer 252
TLS-SRP 273–274
TLS-stripping attack 233, 241
TOCTOU, *see*: time-of-check time-of-use
TOFU, *see*: trust on first use
token, *see*: authentication token
Top Secret, *see*: classification level
Torpig (botnet) 204
touch (command) 136
traffic normalization 333
training (education), *see*: education
training (IDS) 314–315
trampoline function 198, 208
transient phishing site 271
transitive trust 23, 221, 234, 297
transport mode (IPsec) 299, 301–302
transposition cipher 51
trawling 57, 60
tree authentication, *see*: Merkle authentication
Tribal Flood Network (TFN, TFN2K) 325, 334
trinoo (DDoS) 325, 334
triple-DES (3DES) 49–51, 274
Tripwire (file change detection) 43, 190
Trojan horse (malware) 152, 186, 194, 196, 207
true negative rate (TNR) 312–313
true positive (TP) 312
true positive rate (TPR) 312
trust agility 24, 234
trust anchor (PKI) 24, 217–220, 223–230, 232–234, 237–239, 254
trust anchor justification 220
... *see also*: design principles
trust anchor list 227, 229
trust but verify 24
trust domain 12, 149
trust management 220
trust models, *see*: certificate trust models
trust models (SSH), *see*: SSH (trust models)
trust on first use (TOFU) 220, 231, 241, 294, 306
trusted 4
... certificate 229
... certificate store 219, 223, 254
... computing 214
... login hosts 297
... server 96, 113, 222–223, 237
... trusted path (input/output) 71–72, 267, 273, 275
trusted third party (TTP) 113, 215
... *see also*: CA, identity provider, KDC, KTC, RA
trusted vs. trustworthy 4
trustworthy 4, 27, 224, 251
TTL field (time-to-live) 300–301, 305–306, 326
TTP, *see*: trusted third party
tunnel (encrypted) 250–251, 253, 282, 286, 290, 292–293, 297–300, 303, 306
tunnel mode (IPsec) 299, 301–302
tunneling (protocol) 250, 286, 288, 295, 298, 302
tunneling a port 295
two-factor authentication (2FA) 67–70, 86, 287
two-stage authentication 70, 72
two's complement (binary representation) 160–166, 178
type casting (C) 160–163, 173
type conversion 159–163
type promotion 160–163
type safety (type-safe language) 160, 173
typing rhythm, *see*: biometric modalities
typosquatting 270
- ## U
- UDP (User Datagram Protocol) 283, 285, 290, 300, 304–306, 326, 334
... amplification 324
... flood 323, 325, 334
... packet forwarding 290
UID 129, 134, 137, 150, 157
... effective UID (eUID) 137
... UID 0 vs. kernel 175
ugo permission model, *see*: user, group, other
umask (protection bits) 135–136
unauthenticated key establishment 93–94, 102–104, 109
undecidable problem 189, 208
underground economy 208
Unicode, *see*: character encoding
unilateral authentication 93–94, 112, 223
Unix 126, 131, 133, 151, 167, 176–177, 188, 198, 207, 292–293, 297, 327, 333
... security 207
... viruses 208
unknown key-share attacks 120

- unlink (system call) 158
 - unmotivated user 273
 - unqualified name 247
 - unsigned integer (C) 161–166
 - update 186, 194–195, 204, 216–217, 314, 317–318, 325
 - URI 247, 249–252, 256–259, 265–266, 275
 - URI reserved characters 266
 - URL 246–252, 255, 258, 263, 270
 - ... syntax 247
 - URL bar (address bar) 230–232, 237, 247, 270–271
 - usability and security 8, 23, 70–71, 75, 87, 220, 240–241, 269–275, 285, 287, 311, 339–340
 - ... design principles 273
 - ... evaluation methods 340
 - ... user compliance 23, 26
 - use-after-free (memory) 179
 - user (file owner) 134–136
 - user acceptance, *see*: user buy-in
 - user agent 249
 - user authentication 56–87
 - ... categories 70
 - user buy-in 23, 75, 240, 273
 - ... *see also*: design principles
 - user, group, other (ugo) permission model 134, 136
 - user interface (UI) 273
 - user mode vs. kernel 195, 198–199, 208
 - user space (memory layout) 166–167, 175, 195
 - user space vs. kernel memory 195, 197–198
 - user studies (formal) 340
 - user workflow 12
 - userid, *see*: UID, username
 - username (account name) 56, 129
 - /usr/bin/passwd (password command) 137, 176
 - UTF-8 (character encoding) 265–266
 - UTF-16 (character encoding) 265–266
 - UTF-32 (character encoding) 265–266
- V**
- vault (password) 77
 - VAX (computer) 193
 - Venn diagram 313
 - verifiable text 60, 98, 106–109, 111–112, 120
 - verifier 93
 - Vernam cipher, *see*: stream cipher
 - version detection 318
 - violation of security policy 5
 - virtual circuit 289
 - virtual machines 208
 - virtual memory address 126, 128, 149, 152
 - virtual private network (VPN) 224, 282, 287, 297–303, 306
 - ... architecture 299
 - ... designs 299
 - ... use cases 299
 - virtual table (vtable), *see*: dispatch table
 - virtual terminal connection, *see*: telnet
 - virus 185–192, 207
 - ... alternate definition 188
 - ... anti-detection 191–192
 - ... boot sector 188–189
 - ... companion 188
 - ... data file 189
 - ... detection in practice 190, 207
 - ... email 189, 205
 - ... macro 189, 291
 - ... metamorphic 191–192
 - ... polymorphic 191
 - ... primer 207
 - ... program file 187
 - ... shell script 188
 - ... undecidable problem 189
 - visual deception 270
 - voice authentication, *see*: biometric modalities
 - VPN, *see*: virtual private network
 - vulnerability 5, 320
 - vulnerability assessment 11, 27, 179, 311, 317–318, 333
 - vulnerability scanners 317–320, 333
- W**
- WannaCry (ransomware) 202–203, 208
 - Ware report (1970) 152
 - waterfall model, *see*: lifecycle (of software development)
 - weak link 23, 50, 66, 233
 - weak password subspaces 87
 - weak secret 66, 68, 92, 95, 98, 106, 111–113
 - weak type safety (weakly-typed) 160, 173
 - web application firewalls 306
 - web application security 275
 - web architecture 267
 - web form (HTML) 248–250, 261–262, 264, 267
 - web hosting (site hosting) 234
 - web of trust, *see*: PGP
 - web origin, *see*: origin (SOP)
 - web security 246–273, 274–275
 - web site identity 272
 - web SSO, *see*: federated identity system
 - web templating frameworks 275
 - webmail interfaces 238, 240, 260
 - weird machine 341
 - what you are 69–71
 - what you do 71
 - what you have 67, 69–70
 - what you know 69–70
 - WhatsApp Messenger 225
 - where you are 69–70
 - white-box, *see*: black-box vs. white-box
 - white-hat, *see*: black-hat vs. white-hat

whitelist, *see*: blacklist vs. whitelist
why security is hard 25–27, 120, 339
Wi-Fi (IEEE 802.11) 13, 300, 327
widget (web) 201
wildcard domain 230
window object (HTML) 251, 255–256, 258–260, 270
window.document 255
window.location 251, 255
window.open 258
Windows (OS) 113, 151, 156, 177–178, 189, 198–
199, 202, 208, 293, 319, 327
... function hooking 198
WinDump 319
WireGuard (VPN) 303
wireless access point 250, 287, 297, 327
Wireshark (Ethereal) 319
work factor 23
working key, *see*: key
world-writable file 139–140, 158
worm 185–187, 190–194, 207
... flash worm 193, 208
... incidents 191, 193–194
... self-stopping 190
... spreading techniques 187, 191–194, 201, 208
wrap around (integer) 161–162, 165
wrapper function 176, 198
write permission (W), *see*: permissions

X

X Window System (version 11) 296
... X11 (forwarding) 294, 296
X.500 224, 233
X.509, *see*: certificate
XMLHttpRequest 260, 275
XMPP (Extensible Messaging and Presence Protocol) 254
XOR (exclusive-OR) 33–35
Xprobe2 (OS fingerprinting) 318, 333
XSS, *see*: cross-site scripting

Y

Yahoo! 194
Ylönen, Tatu (SSH inventor) 297, 306

Z

Zeek (Bro) 315–316, 319, 332–333
Zenmap (Nmap UI) 318–319
zero extension (integer) 161–163
zero-day exploit 190, 204
zero-knowledge, *see*: proof of knowledge
zero-pixel (window, iframe) 201, 262
Zeus (bank Trojan) 204