

Index

802.3, *see*: IEEE 802.3
 802.11, *see*: IEEE 802.11
 802.1X, *see*: IEEE 802.1X

A

abortive release (TCP) 304
 access (system call) 157–158
 access attributes 130
 access control **3**, 6, 126, 134, 142, 195, 202, 214, 257, 282, 298
 ... access control list, *see*: ACL
 ... capabilities list (C-list) 131–133, 150
 ... capability 65, 132–133, 151
 ... discretionary (D-AC) 144, 151
 ... mandatory (M-AC), *see*: M-AC
 ... ticket (capability) 132–133
 access control (802.11 network) 341–342, 348, 367
 ... dual-port model, *see*: IEEE 802.1X
 ... failure (WEP), *see*: WEP (access control failure)
 ... link layer, *see*: link-layer access control
 ... physical basis 347
 ... port-based, *see*: IEEE 802.1X
 ... unauthorized network access 347
 ... upper-layer, *see*: upper-layer authentication
 ... wireless 347
 ... *see also*: perimeter defense
 access control entry, *see*: ACE
 access control indicator 128–129, 133, 149
 access control matrix **130**–132, 149, 151–152
 access matrix, *see*: access control matrix
 access point (802.11), *see*: AP
 account 56
 ... account recovery 13, 58, 64–**65**, 67, 73, 262
 accountability 3–**4**, 23, 129, 133, 234
 ACE (access control entry) 130–132, 149
 ACK flag 284–285, 304
 ACK storm 331
 acknowledgement number (TCP) 305, 329–330
 ACL (access control list) 131–134, 136, 149, 151
 ACME (certificate management) 230, 270
 active attack, *see*: attack
 active content 185, **200**, 246, 248, 259–260, 286
 ActiveX controls 200, 259
 ad hoc mode (802.11) 341
 address (Bitcoin) 377–**378**, 380, 382–383, 397–398
 ... data-encoding address 383
 ... per-transaction address 378–379
 ... *see also*: P2PK, P2PKH, P2SH
 address bar, *see*: URL (bar)
 address resolution attacks 185, 204, **325**–329
 Address Resolution Protocol, *see*: ARP
 Address Space Layout Randomization, *see*: ASLR
 address spoofing, *see*: IP address (spoofing)
 Administrator (Windows) 156
 Adobe Flash 194, 200, 259
 Adobe PDF 189
 Adobe Reader 259
 Advanced Encryption Standard, *see*: AES
 adversary (opponent) 5, 25
 ... classes, *see*: adversary model
 adversary model 8–11, 19, 27, 320, 412
 ... 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 (Advanced Encryption Standard) 21, **34**, 48–51, 203, 254, 274, 361
 AES-CCMP (CCM protocol) **361**–362, 364–365
 ... CCMP header (802.11) 361–362
 ... counter block 362
 ... frame encryption 361–362
 ... KCK (key confirmation key) 363, 365–366
 ... KEK (key encryption key) 363, 365–367
 ... key hierarchy (session key derivation) 363
 ... KeyID field, *see*: MAC frame (KeyID field)
 ... mandatory for 802.11-compliant RSN 367
 ... nonce (CTR mode) 361–363
 ... nonce generation, *see*: IEEE 802.11 (nonce)
 ... packet number (PN) 362–363
 ... padding fields (frame format) 362
 ... replay protection 362–**363**, 370
 ... session keys 361, 363
 ... special first block in CBC-MAC 362
 ... TK (temporal key) 363, 366, *see also*: PTK
 AES-GCMP (GCM protocol) 364–365, 369–370
 AH (Authentication Header) **300**–303, 305–306
 Aircrack, *see*: wireless analysis tools
 AirSnort, *see*: wireless analysis tools
 Ajax (Asynchronous JavaScript and XML) 260, 275
 alarm (IDS) 310–315
 alarm imprecision 312–313
 alarm precision 312–313
 algorithm 30
 algorithm agility 24
 allowlist, *see*: denylist vs. allowlist
 ... MAC address 349
 ALU (Arithmetic Logic Unit) 163, 165
 ... ALU flags 163–165, 178
 ... carry flag 164–166, 178
 ... overflow flag 164–166, 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, 378
- antenna (directional, high-gain, omni-directional) 345
- anti-detection (malware) 191
- anti-virus 185, **190**, 197, 313, 320
- ANX (Automotive Network eXchange) 224
- AP (access point, 802.11) 340–341
 - ... access point mapping 345
- API hooking, *see*: hooking
- application-level filter, *see*: firewall
- Argon2 (hashing) 61, 86
- arguments (argv) 177
- Arithmetic Logic Unit, *see*: ALU
- ARM (ARMv7) 151, 178
- ARP (Address Resolution Protocol) 303, **327**, 334, 360
 - ... cache 328
 - ... cache poisoning 328
 - ... tables 328
- ARP spoofing (of MAC address) 316, 325, **328**–329, 331, 334
 - ... defenses 328
- arpspoof (tool) 329
- AS (authentication server, 802.11) **340**–341, 348, 350
- ASCII character 34, 107, 203, 236, 265–266
- ASLR (Address Space Layout Randomization) 170, 173, **179**
- assembly language 163, 208
- asset 4
- associated state (802.11) 342–344
- association (802.11) **342**–343, 346, 348, 353
 - ... request 342–343
- assumptions 11, 16, 18, 24, 27, 71, 165, 412–413
- assurance 19–20
- asymmetric cryptography, *see*: public-key crypto
- atomic transactions 158
- ATT (Automated Turing Test) 80
- attack (approaches, methods) 5, 27, 99
 - ... active vs. passive **32**, 94, 102, 107, 254, 345–346, 360, 368
 - ... 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
 - ... (wireless) message injection 347, 358
 - ... (wireless) replay 347, 364, 370
 - ... (wireless) scanning, *see*: scanning (wireless)
 - ... *see also*: denial of service, dictionary, exhaustive search, impersonation, middle-person, social engineering, WLAN (threats)
- attack libraries 27
- attack models (biometrics) 87
- attack models (ciphers) 32
 - ... chosen-ciphertext 32
 - ... chosen-plaintext 32, 354
 - ... ciphertext-only 32
 - ... known-plaintext **32**, 111, 354–356, 359–360
- 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
- attribute (certificate) 215
- attribution (accountability) 4
- audit log 23, 129, 133, 196, 250, 283, 287, 310–311, 315–316, 332
- audit trail, *see*: audit log
- AUTH TLS 254
- authenticated data structure 403, 406
- authenticated encryption (AE) 36, **47**–49, 51, 253–254, 274, 361, 366
 - ... CCM mode 47–49, 51, 274, 361
 - ... GCM mode 49, 51, 274, 369
 - ... generic composition 47–48
 - ... OCB mode 51
- authenticated key establishment (key exchange) 92, **94**, 105, 120, 253, 294
- authentication **3**, 56, 92, 214
 - ... authentication cookie (browser) 260, 265
 - ... factors vs. signals 70
 - ... in 802.11, *see*: low-level, upper-layer
 - ... remote authentication 71–73, 214
 - ... *see also*: challenge-response, data authentication, entity authentication, user authentication
- Authentication Header (IPsec), *see*: AH
- authentication path, *see*: Merkle path authentication
- authentication protocol 92–94, 97–100
 - ... hybrid 94
 - ... mistakes 97–99
- authentication server (802.11), *see*: AS
- authentication token (authenticator) 65, 69, 113–114
- authentication tree, *see*: Merkle authentication tree
- authentication-only protocols 93, 112
- authenticator (token), *see*: authentication token
- authenticator (802.11) 341, 343, **348**–350
- authenticity 214
- Authenticode (code signing) 208
- authorization 3, 56, 214
- authorship attribution system 405

- auto-rooter (malware) 192, 319
- Automated Turing Test, *see*: ATT
- 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
- badlist, *see*: denylist
- Balloon (hashing) 86
- BAN logic (Burrows, Abadi, Needham) 105, 120
- band (radio spectrum) 342
- bankruptcies/failures (Bitcoin exchanges) 397, 405
 - ... MtGox 397
 - ... QuadrigaCX (Gerald Cotten) 397
- 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
- base58 encoding 378, 397
- bash (shell) 171
- basic constraints (extension) 221
- basic service set (802.11), *see*: BSS
- bastion host 291–292
- Bayesian detection rate 313
- bcrypt (hashing) 61
- beacon (802.11) 341–343, 346
- 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
 - ... failure to capture (failure to acquire) 72
 - ... failure to enroll 72
 - ... 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
- BIP (Bitcoin Improvement Proposal) process 406
- birthday paradox 43–44, 357
- bitcoin (currency unit), *see*: BTC
- Bitcoin (system) 376, 405
 - ... address, *see*: address (Bitcoin)
 - ... append-only ledger 377, 385
 - ... attractive to criminals 202, 396, 399
 - ... block, *see*: block (Bitcoin)
 - ... blockchain, *see*: blockchain (Bitcoin)
 - ... challenges (ongoing) 398, 405
 - ... change 381
 - ... coinbase, *see*: coinbase transaction (Bitcoin)
 - ... compliant behavior 393
 - ... consensus 381, 387, 391–392, 405
 - ... cryptographic algorithms 397, 406
 - ... currency, *see*: BTC
 - ... custodian 397
 - ... deterministic key management, DSA example 398
 - ... exchange 397, *see also*: bankruptcies/failures
 - ... hashing algorithms used 397
 - ... head block 377, 386
 - ... header, *see*: block header (Bitcoin)
 - ... incentives 387, 393
 - ... inventor 405
 - ... master public key property 398
 - ... miner, *see*: miner (Bitcoin)
 - ... mining, *see*: mining (Bitcoin)
 - ... mining bound, *see*: mining bound (Bitcoin)
 - ... multiple signatures 384
 - ... myths 405
 - ... node, *see*: node (Bitcoin)
 - ... opcodes (operation codes) 380, 382–383
 - ... password risks 396
 - ... power consumption (resources) 44, 398
 - ... private key and password management 396–398, 406, *see also*: wallet (Bitcoin)
 - ... private key risks (loss, theft) 396, 399
 - ... reference implementation 388, 393, 406
 - ... regular transaction 379–380, 387
 - ... regular user 395
 - ... script, *see*: script (Bitcoin)
 - ... SIGHASH (signature fields covered) 383
 - ... signature validation 382–383
 - ... signatures (ECDSA) 397–398
 - ... transaction, *see*: transaction (Bitcoin)
 - ... used for smart contracts 406
 - ... used to timestamp data 383
- black-box vs. white-box 10–11, 34
- black-hat vs. white-hat 178–179, 316–318, 320
- blacklist, *see*: denylist vs. allowlist
- blind TCP reset 332
- block (Bitcoin) 377, **384**
 - ... block with transactions 385
 - ... candidate block 386–**387**, 392
 - ... confirmed 388–389, **392**–393, 395
 - ... depth 388–389
 - ... difficulty (relative mining difficulty) 390
 - ... difficulty (leading zeros) 390–391
 - ... height (number) 381, 385, 387–**389**, 391
 - ... mining, *see*: mining (Bitcoin)

- ... model (stack of blocks) 389
- ... number, *see*: block (Bitcoin, height)
- ... orphan block (pool) 392
- ... parent block 387, 392–393
- ... preparation 386–387
- ... production rate 381, 387
- ... reward 381, 388, 392–394
- ... selection as voting 393
- ... side-pool (side-chain) block 392
- ... stale 392
- ... subsidy 381, 388, 401
- ... top block 388–389
- ... unconfirmed 393
- ... unrecognized 392–393
- ... validation checks 391
- block (Ethereum) 392
 - ... block header fields 402
 - ... block header size 403
 - ... difficulty 402
 - ... gasLimit 402
 - ... logsBloom (logs Bloom filter) 402
 - ... mining, *see*: mining (Ethereum)
 - ... number 402
 - ... ommersHash 402
 - ... parent 402
 - ... proof of work 402–403
 - ... receiptsRoot 402
 - ... reward 401
 - ... stateRoot (world state) 402, 404
 - ... timestamp 402
 - ... transactionsRoot 402, 404
 - ... uncle (ommer) 392, 401–402
- block cipher 34
 - ... algorithms, *see*: AES, DES, triple-DES
- block header (Bitcoin) 384, **385**–386, 391
 - ... authenticity 395
 - ... Merkle root, *see*: Merkle root (Bitcoin)
 - ... mining bound, *see*: mining bound (Bitcoin)
 - ... mining nonce 385, **387**–389
 - ... timestamp 385, **387**
 - ... version 385, **387**
 - ... *see also*: block (Bitcoin, preparation)
- blockchain (Bitcoin) xv, 376–377, 384, **385**–386
 - ... branch reorganization 393
 - ... explorer (software tool) 406
 - ... fork (resolution) 393–394
 - ... main branch (main chain) 392–393, 405
 - ... “on the blockchain” 392
 - ... properties 377
 - ... side branch 392
 - ... verifying integrity of 386
- blocklength (cipher) 34
- BlockSci (blockchain explorer) 406
- Blue Pill (rootkit) 208
- Bluetooth 370
- 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
- Bro, *see*: Zeek
- broadcast (address, message) 323, 328
- broadcast address (MAC), *see*: MAC address (broadcast)
- browser
 - ... chrome (border) 270
 - ... cookie, *see*: HTTP cookie
 - ... event 248
 - ... event handler 248–249, 262
 - ... extensions 260
 - ... history 250
 - ... mobile browsers 275
 - ... onclick (browser event) 248
 - ... onload (browser event) 249, 262
 - ... onmouseover (browser event) 248, 265
 - ... padlock, *see*: lock icon
 - ... plugins 259–260, 274
 - ... proxy settings 251
 - ... security 246–275, *see also*: trust models
 - ... session 255, 260
 - ... trust model issues 232–233
- browser instances (vendor products)
 - ... Chrome (Google) 219, 231, 257, 271–272, 275
 - ... Firefox (Mozilla) 232–233, 271
 - ... Internet Explorer (Microsoft) 259
 - ... Safari (Apple) 271
- brute force, *see*: attack
- BSD packet filter (BPF) 319, 333
- BSS (basic service set) 341
- BSS (block started by symbol) 166–167
- BSSID (BSS ID) 342
- BTC (bitcoin, currency unit) 376, 381
 - ... *see also*: Bitcoin (system)
- btc-value (field) 380–381
- bucket brigade attack, *see*: grandmaster postal chess
- buffer overflow attack 156, 163, **166**–167, 179, 333
 - ... defenses 172–174, 179
 - ... heap-based buffer overflow 168–170, 178
 - ... stack-based buffer overflow **166**–168, 178, 193
 - ... *see also*: heap-spraying, return-to-libc, ROP
- buffer overrun, *see*: buffer overflow
- bump in the stack (IPsec) 303
- bump in the wire (IPsec) 303
- Byzantine Generals problem (Lamport) 406

C

- C language 178
 - ... *see also*: integer vulnerabilities
- C# 173
- C++ 160, 164
- CA (Certification Authority) 49, 95, **215**–217
 - ... compromise incidents 232
 - ... CA Revocation List, *see*: CARL
 - ... CA-certificate 221, 225, 229
 - ... intermediate CA **217**–218, 225–226, 231–232, 234, 239
- CA/browser forum 230, 241
- CA/browser trust model 229
 - ... *see also*: certificate trust models
- 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 (CA Revocation List) 223
- casting, *see*: type casting
- CBC (Cipher Block Chaining), *see*: modes of opn
- CBC-MAC, *see*: MAC algorithms
- CCM (counter mode with CBC-MAC), *see*: authenticated encryption
- CCMP (CCM protocol), *see*: AES-CCMP
- CCured 179
- CDN (Content Delivery Network) 234, 241, 254, 325, 334
- 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
 - ... issuer 215
 - ... key usage 221
 - ... online status checking 222, *see also*: OCSP
 - ... policy constraints 218, 221, 228
 - ... pros and cons 237–238
 - ... request 24, 216
 - ... reverse 226, 228
 - ... rogue certificate 233, 241
 - ... 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
 - ... *see also*: Subject (certificate)
- certificate directory 216–217, 229, 237–239
- Certificate Management Protocol, *see*: CMP
- Certificate Practice Statement, *see*: CPS
- certificate profile 217, 241
- certificate revocation 49, **221**–224, 230, 233, 237–238, 240–241
 - ... approaches 222–223
 - ... CRL (certificate revocation list) 222, 239
 - ... CRL distribution point 222
 - ... CRL fragments 222
 - ... CRT (certificate revocation tree) 241
 - ... delta CRL 222
 - ... indirect CRL 241
 - ... partitioned CRL 222
 - ... reasons 221–222
 - ... redirect CRL 241
 - ... timeline 222–223, 241
- Certificate Transparency, *see*: CT
- certificate trust models 224–229, 241, 294
 - ... bridge CA trust model 224–226, 228, 241
 - ... browser trust model **227**, 229–234, 272, 274, 294
 - ... enterprise PKI model 227–228, 239
 - ... forest of hierarchical trees 227
 - ... hierarchy (strict CA) 225–226, 233
 - ... hierarchy (with reverse certificates) 226
 - ... mesh trust models (ring-mesh) 225–228
 - ... network PKI 227
 - ... single-CA trust models 224–225
- Certification Authority, *see*: CA
- certification policy, *see*: policy
- certification request 24, 216–217
- CFB (Cipher Feedback Mode), *see*: modes of opn
- CGI script (Common Gateway Interface) 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, 353, 369–370
- channel (radio) 342
 - ... hopping 346
 - ... number 345
- channel security (TLS, HTTPS) 271, 274
- CHAP (authentication) 369–370
- char data type (C language) 160
- character encoding 265–266, 268–269
- character set 265
- character string (C language), *see*: string

- check on first use (COFU) 220
- checksum 3, 41, 111, 305
- CHERI capabilities 151, 413
- Chernobyl virus (CIH) 189
- chgrp (command) 136
- child process (OS) 137, 171, 175–177
- chmod (command) 136
- chokepoint 21, 285
- chop-chop attack (wireless) 346
- 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 (Certificate Management Protocol) 216, 241
- CMS (Cryptographic Message Syntax) 241
- code account (Ethereum) 399, 402
- 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) 412
- coin (virtual) 376
 - ... owner 378, 382
- coinbase transaction (Bitcoin) **381**–382, 385, 387–388, 391, 394
 - ... output hold 393
- collision (hashing) 42, 44, 51
 - ... collision resistance 42–43, 385, 395
 - ... *see also*: WEP (IV collision)
- 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
- commit (to a value) 385
- 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, 354
- confused deputy 200, 262
- congruence (modular arithmetic, mod p) 38–39, 50, **115**–119, 252
- CONNECT (HTTP request method), *see*: HTTP (CONNECT)
- connection forwarding 293
- connection-oriented 304
- connectionless 304
- connectivity 25
- consensus, *see*: Bitcoin (consensus), Ethereum (consensus), distributed consensus
- content body (email message) 235–236
- Content Delivery Network, *see*: CDN
- content header (email message) 235–236
- content inspection 286, 290–**291**, 299
 - ... *see also*: deep packet inspection
- content scanning (email) 238, 240
- content scanning (HTTPS) 254
- Content Security Policy (CSP) 265, 275
- contextualized signatures (IDS) 333
- contract (Ethereum) 399
 - ... contract account, *see*: code account
 - ... creation 400
 - ... *see also*: smart contract
- control flow (integrity) 161, 169–170, 173–**174**, 179, 208, 315
- control frames, *see*: frame types (802.11)
- cookie (HTTP), *see*: HTTP cookie
- COPS (scanner) 319, 333
- CORS (cross-origin resource sharing) 275
- cost-benefit analysis 8, 174
- counter mode with CBC-MAC, *see*: CCM
- countermeasure 6
- covert channel 29, 152
- cp (copy) 293
- CPS (Certificate Practice Statement) 230
- CRC (Cyclic Redundancy Code) 42
 - ... use in 802.11: 342, 352, 355, 358, 369
 - ... linearity of 356
- credential 100, 113, 264, 271
 - ... credential manager 113

- credentialed scanning 317, 333
 CRL (certificate revocation list), *see*: certificate revocation
 cross-check **24**, 173, 198, 218, 220, 230, 232, 239, 294, 395, *see also*: independent confirmation
 cross-frame communications 274
 cross-origin communications 274
 cross-site request forgery, *see*: CSRF
 cross-site scripting, *see*: XSS
 cross-view difference (rootkit detection) 200
 cruise liner certificate 234
 crypto-strength key vs. weak secret 95
 cryptocurrency xv, 376, 397, 399, 405
 ... bitcoin, *see*: BTC
 ... ether, *see*: ETH
 ... *see also*: Bitcoin, Ethereum, Namecoin
 cryptocurrency vulnerability studies 406
 cryptographic key, *see*: key
 Cryptographic Message Syntax, *see*: CMS
 cryptographic protocol 92, 120, 214
 cryptography 30–53, 92, 214, *see also*: Bitcoin (cryptographic algorithms), WEP (use in RC4)
 CryptoKitties 405
 cryptosystem 31
 cryptovirology (ransomware) 208
 CSRF (cross-site request forgery) **261**–262, 264, 275
 ... defenses 262, 265
 CT (Certificate Transparency) 234
 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 protocol 234
 ... DANE certificate 234
 dangerous error 273
 dangling pointer 179
 DAO (Decentralized Autonomous Org.) 405–406
 DApps (decentralized applications) 405–406
 darknet 206
 data authentication, *see*: data origin authentication
 Data Encryption Standard, *see*: DES
 data execution prevention (DEP), *see*: non-executable
 data extrusion 283
 data flow diagram 12, 14
 data frames, *see*: frame types (802.11)
 data integrity, *see*: integrity
 data link (OSI layer 2) 300, 328
 data origin authentication (data authentication, message authentication) 3–4, 39, **45**–47, 253, 334, 355, 358
 data remanence, *see*: secure deletion
 data segment (OS) 167–168
 data-type validation, *see*: design principles
 database, *see*: SQL
 datablock (filesystem) 138, 140, 142, 157
 datagram 300, 302–305
 DDoS (distributed denial of service) 203, 207, 234, **321**, 325, 333, *see also*: DoS
 ... toolkits 325
 deauthenticate frame (802.11) 344, 346, 360, 369
 debug (command) 194
 decentralized applications, *see*: DApps
 decentralized CA trust 227–228
 decentralized computing platform 376, 399
 decentralized name registration and resolution 405
 deceptive URL (look-alike) 270
 decryption 30–31, *see also*: block cipher, public key cryptography, RSA, stream cipher
 deep packet inspection 287
 default deny (rulesets) 284–285, 287
 ... *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
 demonstration of knowledge, *see*: proof of knowledge
 denial of service, *see*: DoS
 denylist vs. allowlist **21**, 43, 63–64, 85–86, 190, 251, 265, 268–271, 285, 287, 314, 318, 325, 333
 DEP (data execution prevention), *see*: non-executable
 dependability 27
 dependable and secure computing 27, 184
 derivation function (keys), *see*: KDF, PRF
 DES (Data Encryption Standard) **32**, 49, 51
 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 validation P15: **23**, 25, 165, 173, 265, 333
 ... defense in depth P13: **23**, 50, 64, 66, 70, 73, 78, 233, 287, 291, 358
 ... design for evolution HP2: **24**, 60
 ... evidence production P14: **23**, 234, 311, 316
 ... independent confirmation P18: **24**–25, 43, 70, 218
 ... 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, 358
- ... open design P3: **21**, 24, 31, 41, 80, 358
- ... reluctant allocation P20: **24**, 262, 323–324
- ... remnant removal P16: **23**, 104, 144
- ... request-response integrity P19: 21, **24**, 158, 218, 325, 328, 334
- ... safe defaults P2: **21**, 206, 224, 233–234, 273, 284–285, 358
- ... 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
- ... WEP (failure of design principles) 358
- design principles for usable security 273
- desynchronization (TCP session) 331
- DET (detection error tradeoff) 74–75
- detached signatures (S/MIME) 238
- detection error tradeoff, *see*: DET
- detection rate (true positive rate) 312
- detection vs. prevention 19, 23, 311
- detour patching 198
- device fingerprinting 70, 80
- device pairing methods 120
- Device Provisioning Protocol (802.11), *see*: DPP
- DH (Diffie-Hellman) key agreement 38, 50–51, 93–94, **100**–103, 109–110, 115–121, 236, 252, 274, 300, 306, 323, 367
- ... DHE (DH ephemeral) 252–253
- ... parameter checks 118–119
- DHCP (Dynamic Host Configuration Protocol) 327
- dial-up session 345
- Diameter (RADIUS alternative) 370
- dictionary attack 57, 60, 63–64, 86, 92, 97–99, **107**–111, 358–359, 367–368
- Diffie-Hellman, *see*: DH key agreement
- digital collectibles 405
- digital evidence, *see*: evidence
- digital notarization 405
- 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
- disassociate frame (802.11) 344–346, 367, 369
- discrete logarithm 50, 101, 117, 121
- disk encryption 200, 208
- dispatch table 169, 197–198
- distance-bounding protocols 98
- distinguished name, *see*: DN
- distributed consensus (Lamport) 406
- distributed denial of service, *see*: DDoS
- distribution system (802.11), *see*: DS
- diversity of code 22
- DKOM (direct kernel object manipulation) 198
- DLL (Dynamically Linked Library) 198–199
- ... injection, *see*: injection (DLL injection)
- DMA (Direct Memory Access) 199
- DMZ (demilitarized zone) 285, 291–292
- DN (distinguished name) 215
- DNS (Domain Name System) 235, 246–247, 282, 284–285, 291–292, 300, 304, 306, **325**, 334
- ... attacks on (listed by domain exploited) 327
- ... authoritative DNS name server 326–327
- ... 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 loading (HTML) 248
- document object (HTML), *see*: DOM
- ... document.cookie 256, 263, 265
- ... document.domain 255, 259
- ... document.getElementById 263
- ... document.location 255, 263
- ... document.URL 255
- ... document.write 248, 265
- DOM (Document Object Model) 255, 274
- domain, *see*: protection domain
- Domain (cookie attribute) 255–256, 259
- domain filtering 271
- domain mismatch error 232
- domain name (DNS) 247
- Domain Validated certificate, *see*: DV certificate
- DoS (denial of service) 3, 6, 15, 24, 187, 193, 284, **320**–325, 328, 333–334
- ... defenses 325

- ... motives 320
 - ... on revocation 223–224
 - ... via rogue AP 345
 - ... wireless 346–347, 369
 - ... radio jamming 346
 - ... service attack 346
 - double-free (memory management) 179
 - double spending 379, 393, 395
 - downloader, *see*: dropper
 - downloader graph 201, 208
 - DPP (Device Provisioning Protocol) 368
 - Dragonblood (attack, 802.11) 370
 - Dragonfly (key establishment protocol) 368–370
 - ... side channel attack 370
 - drive-by download 170, 185, 200–201, 207–208, 252, 265, 286
 - dropper (malware) 201–202, 208
 - DS (distribution system, 802.11) 340–341
 - 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
 - dual-port access control, *see*: IEEE 802.1X
 - DV (Domain Validated) certificate **229**, 231, 270–272
 - dynamic analysis 173
 - dynamic linker, *see*: linking and loading
 - dynamic memory allocation 169
 - dynamic packet filter 284, 286–287, 306
- ## E
- e-cash (electronic cash) 379
 - EAP (Extensible Authentication Protocol) 347, **349**–350, 369–370
 - ... key management framework and hierarchy 369
 - ... messages 348–349
 - ... over LAN, *see*: EAPOL
 - EAP method (802.1X) 348–349, **368**, 370
 - ... method categories 368
 - EAP-EKE 369
 - EAP-FAST 369
 - EAP-GTC (generic token card) 369
 - EAP-over-RADIUS 350, 369
 - EAP-PSK 369
 - EAP-pwd 369–370
 - EAP-TLS 349, 368–369
 - EAP-TTLS 369
 - EAPOL (EAP over LAN) 349–350
 - ... EAPOL-Key messages 365
 - Easter egg (software) 205
 - Easy Connect (WFA), *see*: WFA
 - eavesdropping 18, **31**, 67, 94, 101–102, 196, 238, 297
 - ... wireless 347, 353
 - EC, *see*: elliptic curve, *see also*: ECDSA
 - ECB (Electronic Codebook Mode), *see*: modes of operation
 - ECDSA (elliptic curve DSA) 51, 253
 - ... public key 378, 397–399, 406
 - ... public key, compressed format 398
 - ... curve equation 398
 - ... secp256k1 (curve instance) 398, 406
 - echo request (echo reply), *see*: ping
 - EdDSA (Edwards-curve DSA) 253
 - education (training) 25–26, 79, 185, 269, 271, **273**
 - eduroam (802.1X-based authentication) 370
 - Edwards-curve DSA, *see*: EdDSA
 - effective key space, *see*: key space
 - effective UID (eUID), *see*: UID
 - egress filtering 284–285, 323, **324**–325
 - EKE (encrypted key exchange) 94, **105**, 107–110, 120, 369
 - elevation of privilege, *see*: privilege escalation
 - ElGamal encryption 101
 - ElGamal key agreement 101
 - elliptic curve (EC)
 - ... cryptography (ECC) 50–51, 252–253
 - ... DH ephemeral (ECDHE) 252
 - ... Digital Signature Algorithm, *see*: ECDSA
 - 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), *see*: ESP
 - encapsulation 288, **298**, 300, 302
 - ... “runs over” terminology 349
 - encrypted filesystem 200
 - encrypted key exchange, *see*: EKE
 - encryption 30–39
 - ... hybrid encryption **38**, 203, 236
 - ... in-RAM 200
 - Enhanced Open (WFA), *see*: WFA
 - Enigma machine 51
 - enterprise SSO 113–114

- entity 4, 15, 92, 104
 - entity authentication 3, **92–93**, 100, 104
 - entity encoding 265–**266**
 - entropy (Shannon entropy) 81–87
 - envelope (email) 235–236
 - envelope method of hashing, *see*: secret prefix
 - environment variables (envp) 167, 169, 177, 188
 - EOA (externally-owned account) 399, 402
 - 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
 - ESP (Encapsulating Security Payload) **300–306**
 - ESS (extended service set), 341, 346
 - ESSID (ESS ID) 342, 346
 - /etc/group 134
 - /etc/hosts.equiv 194, 297
 - /etc/passwd 57, 60, **134**, 157–158, 194, 267
 - /etc/shadow (shadow password file) 134
 - ETH (ether, currency unit) 399–400
 - ... *see also*: Ethereum (system)
 - Ethash (hashing) 404, 406
 - ether, *see*: ETH
 - Ethereal, *see*: Wireshark
 - Ethereum (system) 376, **399**, 402
 - ... account balance 399, 402
 - ... acctStorageRoot 399–400, 404
 - ... address 399–402, 404
 - ... block header fields, *see*: block (Ethereum)
 - ... blockchain 402
 - ... Bloom filter 401
 - ... candidate block 402
 - ... codeHash 399–400
 - ... consensus 402–403, 405, *see also*: GHOST
 - ... currency, *see*: ETH
 - ... currency production end-date 401
 - ... decentralized consensus 404
 - ... forks (blockchain) 403
 - ... gas, *see*: gas (Ethereum)
 - ... main-chain block 402
 - ... message (internal transaction) 399–400, 402, 406
 - ... nonce 399–403
 - ... overview of components 402
 - ... papers (white, yellow, beige) 406
 - ... persistent state 399
 - ... production rate (blocks) 403
 - ... programming languages 404
 - ... replicated state machine 404
 - ... reward (for mining), *see*: block (Ethereum)
 - ... smart contract, *see*: smart contract
 - ... starting balance 400
 - ... transaction, *see*: transaction (Ethereum)
 - ... types of accounts 399
 - ... virtual machine, *see*: EVM
 - ... world state 403–404
 - Ethernet 300, 304, 316–317, 327–328, **340**
 - Ethernet ports (controlling access), *see*: IEEE 802.1X
 - ethical hacking 156
 - ... *see also*: responsible disclosure
 - Ettercap 328–329, 331, 334
 - Euler phi function (ϕ), *see*: phi function
 - EV (Extended Validation) certificate **230–231**, 241, 270–272
 - ... guidelines 230, 241
 - evasive encoding (HTTP, HTML) 265–266
 - event (security) 7, 82, 310–313, 315
 - event (browser), *see*: browser (event)
 - event outcomes (IDS) 311–312
 - event space 82
 - evidence 3, 311
 - evidence production, *see*: design principles
 - EVM (Ethereum virtual machine) 400
 - ... execution logs 401
 - ... execution memory 400
 - ... gas (fee schedule), *see*: gas (Ethereum)
 - ... machine state (local) 400
 - ... opcodes 401
 - ... run-time stack 400
 - ... storage (persistent) 400
 - exclusive-OR, *see*: XOR
 - exec (system call) 137–138, 171, 176–**177**
 - ... execl 171, 177
 - ... execve 176–177
 - executable content, *see*: active content
 - execute permission (X), *see*: permissions
 - 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, 350, 352
 - exposure maps (network monitoring) 333
 - extended service set (802.11), *see*: ESS
 - Extended Validation certificate, *see*: EV certificate
 - Extensible Authentication Protocol, *see*: EAP
 - extension field, *see*: certificate (extension fields)
 - external penetrator 332
 - externally-owned account (Ethereum), *see*: EOA
 - extrusion detection 333
- ## F
- facial recognition, *see*: biometric modalities
 - fail closed vs. fail open **21**, 224, 233–234
 - fail-safe 21
 - failures (definition) 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
 - FAT (file allocation table) 189
 - fault tree analysis 27
 - faults 27
 - favicon 271
 - federated identity system 113–114, 120
 - feedback to user 273
 - fiat currency xv, 397
 - FIDO (authentication) 86
 - file (filesystem) 126, 128, 138
 - ... file ACL 136
 - ... file allocation table, *see*: FAT
 - ... file descriptor 158, 177, 304
 - ... hidden filename extension 205
 - file locker (malware) 202–203
 - file metadata, *see*: inode
 - file-based access control 133–134
 - filename resolution, *see*: name resolution
 - filename squatting attack 159
 - 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
 - ... (meaning: hash), *see*: hash value
 - ... cross-check 218, 220, 232, 241, 294
 - ... recognition, *see*: biometric modalities
 - ... *see also*: device fingerprinting, OS fingerprinting
 - finite field
 - ... computational aspects 369
 - ... polynomials over 356
 - ... finite-field cryptography (FFC) 50, 252
 - Finney, Hal (Bitcoin) 405
 - 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
 - ... hybrid appliance 287
 - ... internal 291
 - ... limitations 286
 - ... packet filter 282–288, 306
 - ... packet-filtering rules 283–**285**, 306
 - ... personal (host-based) 287–288
 - ... proxy (circuit-level) 286–288, **289**–292, 306, 325
 - ... proxy historical context 306
 - ... web application firewall 306
 - flag bits (TCP header) 304–305
 - Flask security architecture 145
 - Flash cookie 259
 - flash crowd 334
 - flooding attack (DoS) **320**–321, 323, 331, 333
 - Fluhrer, Mantin, Shamir, *see*: FMS attack
 - FMS attack (WEP keys) 353, **359**–360, 369
 - forensic analysis 23, 129, 133, 200, 287, 311, 316, 333
 - Foreshadow (hardware side channel) 413
 - fork (system call) 137, 158, 171, **176**–177, 296
 - form (HTML), *see*: web form
 - ... form tag 248
 - formal analysis methods 411
 - 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, 368
 - four-pass handshake (802.11) 348–350, 359, 363, **365**–368, 370
 - ... forcing nonce reuse (attack) 370
 - fragment (packet) 290, 304–306, 321
 - fragmentation (802.11) 360, 362
 - fragmentation attack 290, 333, 360
 - frame (data, Ethernet) 300, 303–304, 316, 328
 - frame (HTML) 201, 255, 257–260, 274
 - ... inline frame (iframe) 258
 - frame pointer (FP) 167
 - frame types (802.11) 341
 - ... control frames 341
 - ... data frames 341
 - ... management frames 341
 - 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
 - ftapv (GCC compiler option) 166
 - fully qualified domain name (FQDN) 247, 249, 258
 - function call sequence (C language) 167
 - function hooking, *see*: hooking
 - function pointer 169–170
 - fuzz testing (fuzzing) 179, 333
 - fuzzy commitment 45
- ## G
- gait, *see*: biometric modalities
 - gas (Ethereum) 400

- ... fee schedule 400–401, 406
 - ... gasPrice, gasLimit 400–403
 - ... intrinsic gas costs 401, 403
 - ... out of gas (OOG) 403
 - gate extension 147–148
 - gate list 147
 - gateway **250**, 282–292, 297–299, 302, 311, 325
 - gcc (GCC) 158, 164, 166
 - GCM (Galois counter mode), *see*: authenticated encryption
 - GCMP (GCM protocol), *see*: AES-GCMP
 - generative attack (applied to biometrics) 87
 - generator (group) 115–116
 - genesis block (Bitcoin) 377, **385**–386, 390, 392, 396, 405
 - geolocation 70–71, 87
 - GET (HTTP request method) **249**–250, 261–263, 274
 - getfacl (command) 136
 - GHOST (greedy heaviest-observed sub-tree) 406
 - ... *see also*: heaviest-observed chain
 - GID, *see*: group (groupid)
 - GMK (group master key, 802.11) 366
 - GNU C library 179
 - GNU Privacy Guard (GPG) 239
 - goals of computer security 2–4, 24
 - goodlist, *see*: allowlist
 - 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 (groupID), *see*: group (groupid)
 - ... group permissions 136
 - ... groupid (GID, groupID) 134, 137
 - group key (802.11) 342, 352, **366**–367
 - ... Group Key Handshake 367
 - ... *see also*: GMK, GTK
 - GTK (group temporal key, 802.11) 365, **366**–367
 - ... key distribution 366
 - guessing, *see*: password guessing
 - guessing function (guesswork) 84–85
 - ... guess count 85–86
 - ... guess number 84
 - ... guessing index 84
- ## H
- hacker vs. cracker 10
 - hand geometry, *see*: biometric modalities
 - handover (802.11) 341
 - Happy99 (worm-virus) 205
 - hard link 142–144, 157
 - hardening a system 287, 291
 - hardware redundancy 234, 325
 - hardware rings 150–152, 199
 - hardware security 19, 152, 185, 197, 413
 - ... 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, *see*: collision resistance
 - ... GPU hashing 61, 86
 - ... iterated hashing 60, 64, 86
 - ... one-way 41–42, 69
 - ... second-preimage resistant 42
 - ... specialized for passwords 61
 - ... used within digital signature process 44
 - hash pointer, *see*: hashlink
 - hash tree, *see*: Merkle authentication tree
 - hash value (hash) 24, **41**, 232, 239, 241, 294, 385
 - Hashcat, *see*: oclHashcat
 - hashing algorithms 44, 61
 - ... *see also*: Argon2, Balloon, Bitcoin (hashing), bcrypt, Ethash, Keccak, MD5, RIPEMD160, scrypt, SHA
 - hashing target (Bitcoin) 385, 389–390
 - ... *see also*: mining bound (Bitcoin)
 - hashlink (hash pointer) **377**, 385–386, 392, 403, 406
 - HD wallet, *see*: wallet (Bitcoin)
 - heap memory 166
 - ... heap allocator, *see*: secure heap allocator
 - ... heap metadata 169, 173, 179
 - heap spraying (attack) 168–170, 179, 200
 - Heartbleed incident 234, 241
 - heaviest-observed chain 402–403, 405–406
 - heuristic evaluation (usability) 412
 - hijacking 94, 197, 329
 - ... based on address resolution (ARP, DNS) 325–329
 - ... function calls, *see*: hooking
 - ... HTTP session 260, 329
 - ... system calls, *see*: hooking
 - ... TCP session 329–332, 334
 - ... TCP session (mitigation) 332
 - ... WLAN session (association) 344–347, 369
 - HMAC, *see*: MAC algorithms
 - honeypot (IDS) 196, 333
 - ... HoneyD 333
 - hooking 189–190, 196–200
 - host 247
 - ... hostname **247**, 258, 325–327
 - hosts file (local DNS name resolution) 326
 - hotel safebox 16
 - href attribute (HTML) 247–248, 263
 - HSTS (HTTPS strict transport security) 241
 - HTML (Hypertext Markup Language) 200, **247**–248
 - ... document 246, 255
 - ... email 201, 205–206, 238, 261, 264
 - ... form, *see*: web form

- ... HTML5 260, 274
 - ... hyperlink **247**–248, 270
 - ... parsing 248, 264–265, 274–275
 - ... special characters 266
 - HTTP (Hypertext Transfer Prot.) 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
 -htdigest file (digest authentication) 100
 - ... proxy (abuse) 251, 261, 274
 - ... proxy server 234, 249, **250**–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
 - ... Cookie (HTTP header) 255
 - ... injection 274
 - ... navigator.cookieEnabled 256
 - ... persistent cookie 255–256, 260, 262
 - ... protection and pitfalls 261
 - ... same-origin policy, *see*: SOP (SOP for cookies)
 - ... theft 260–263, 265, 329
 - ... third-party cookies 257
 - ... viewing cookies 257
 - ... *see also*: Flash cookie, SYN cookie
 - 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, *see*: HSTS
 - HTTPS-PAKE 273–274
 - hub 316
 - hub-and-spoke model 96, 225
 - human factors 26–27, 411
 - human-in-the-loop, *see*: CAPTCHA
 - ... *see also*: usability and security
- I**
- IAT (Import Address Table) 198
 - IBSS (independent basic service set) 341
 - ICMP (Internet Control Message Protocol) 283–285, 300, 304, **305**–306, 318–319
 - ... destination unreachable 283, 305, 323
 - ... flood 323, 325
 - ... related attacks 324–325
 - ICV (integrity check value, WEP), *see*: WEP (ICV)
 - identification 56, 76
 - identify friend-or-foe, *see*: IFF
 - identity 3
 - ... identity theft 269, 271
 - identity provider (IdP) 113
 - IDES (Intrusion Detection Expert System) 332
 - IDS (intrusion detection system) 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
 - ... metrics 312
 - ... network-based (NIDS) **311**, 315–316, 320, 332
 - ... network behavior and analysis system (NBA)
 - ... rule-based anomaly detection 332
 - ... signature-based 314, 332–333
 - ... specification-based 314–315, 333
 - ... wireless-based 320
 - IE (information element, 802.11) **343**, 353, 365–366
 - IEEE 802.3 340
 - IEEE 802.11 340–343
 - ... 802.11ac 365, 370
 - ... 802.11ax 365
 - ... 802.11b 347, 356, 365
 - ... 802.11g 347, 365
 - ... 802.11i 350, **364**–365, 367, 369–370
 - ... 802.11n 365
 - ... 802.11w 344, 365
 - ... AES-CCMP, *see*: AES-CCMP
 - ... authentication server, *see*: AS
 - ... authenticator, *see*: authenticator (802.11)
 - ... cipher suites 365, *see also*: CCMP, GCMP, TKIP, WEP
 - ... connection state 343
 - ... device driver 349
 - ... fragmentation, *see*: fragmentation (802.11)
 - ... key management (void) **350**, 357, 360–**361**, 364, *see also*: session keys (802.11)
 - ... key management best practices (RFC) 369
 - ... MAC frame, *see*: MAC frame (format)
 - ... nonce generation 365
 - ... original version 350, 365
 - ... port, *see*: port (802.11)
 - ... protected bit 367, *see also*: WEP bit
 - ... radio transmission rates 365
 - ... requestor 348
 - ... RFCs related to security 369
 - ... security evolution 364–365
 - ... security options, *see*: IE (information element)
 - ... timeline of versions 365
 - ... WEP frame, *see*: WEP (frame format)
 - IEEE 802.1X 343, 370
 - ... access control (network access) 348

- ... authentication method, *see*: EAP method
- ... dual-port access control **348**, 367
- ... management and authentication framework 347
- ... model 341
- ... mutual authentication 365, 367
- ... port controller 348–349
- ... port-based access control 348, 370
- ... used with Ethernet ports 348
- ... *see also*: upper-layer authentication
- IETF (Internet Engineering Task Force) 369
- IFF (identify friend-or-foe) 98
- 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
 - ... *see also*: spoofing
- implicit key authentication 104–105
- Import Address Table, *see*: IAT
- in-band signaling 218
- inbound (packet) **283**–292, 304, 333
- independent basic service set (802.11), *see*: IBSS
- independent channel 24, 67, 95, 294
- independent confirmation, *see*: design principles
- index of coincidence (cryptanalysis) 51
- Individual Validated certificate, *see*: IV certificate
- infection vector 207
- information 82
- information element (802.11), *see*: IE
- information-theoretic security 33, 42, 81
- infrastructure mode, *see*: WLAN (infrastructure mode)
- ingress filtering 284–285, 323, **324**–325, 334
- inheriting UID 137–138, 176
- initial keying material, *see*: keying material
- initialization vector, *see*: IV (initialization vector)
- 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, 347, 413
- 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 language) 160
- integer factorization 50
- integer vulnerabilities (C language) **159**–166, 178
 - ... categories 162–163
 - ... extension value change 162–163
 - ... integer overflow 161–164, 178
 - ... integer truncation 161–163, 165
 - ... integer underflow 162–163
 - ... intentional overflow 165
 - ... narrowing loss 162–163
 - ... signedness mismatch 159–163
- integrity (data) **3**, 24, 33, 35, 39, 43, 45, 47
 - ... file checker, *see*: Tripwire
 - ... mechanisms 47
 - ... of public key 37, 214
- integrity check value, *see*: ICV
- integrity mechanism failure, *see*: WEP (ICV failure)
- Intel (x86, IA-32) 151, 166, 178
- intelligent packet filtering 283
- interface design, *see*: usability and security
- interleaving attack, *see*: attack
- 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
 - ... system, *see*: IDS
- intrusion prevention system, *see*: IPS
- 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
- IPS (intrusion prevention system) 311, 317–318
- IPsec (Internet Protocol security suite) 224, 298–299, **300**–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 (Internet Security Association and Key Management Protocol), *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
 - iterated hashing, *see*: hash function
 - IV (Individual Validated) certificate 230
 - IV (initialization vector) 35, 49, 301
 - ... use in AES-CCMP, 361
 - ... use in WEP, *see*: WEP (IV)
 - ... reuse in WEP, *see*: WEP (IV reuse)
- ## 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 (Just Fast Keying, IKE alternative) 306
 - JohnTheRipper (password cracker) 64
 - JSON (JavaScript Object Notation) 275
 - ... JSONP (JSON with padding) 275
 - jump table 169
- ## K
- Kaminsky attack (DNS) 327
 - Kasiski method 51
 - KCK (key confirmation key), *see*: AES-CCMP (KCK)
 - KDC (key distribution center) 96, 114, 237
 - KDF (key derivation function) **61**, 101, 106, 252, 274
 - ... HKDF (HMAC-based KDF) 274
 - ... PBKDF2 61, 64
 - Keccak (hashing) 44, 399, 406
 - KEK (key encryption key), *see*: AES-CCMP (KEK)
 - Kerberos 94, 96, 99, 113–**114**, 120, 294
 - Kerckhoffs’ principle 21
 - kernel
 - ... CPU mode, *see*: supervisor
 - ... functionality 199
 - ... memory **176**, **195**, 197, 199
 - ... module installation 199
 - key 22, 30
 - ... backup and archival 37, 217
 - ... decryption 31
 - ... escrow 238
 - ... good key 104, 120
 - ... master key 252–253
 - ... public-private key pair 37
 - ... recovery 217
 - ... registration 95
 - ... resumption 254
 - ... reuse 33, 48, 51, 68, **95**, 100–101, 104
 - see also*: WEP (IV reuse, keystream reuse)
 - ... session key properties 104
 - ... session key vs. long-term 38, **93**–95, 104, 120, 253
 - ... size 34
 - ... symmetric key 32, 93
 - ... working key (TLS session key) 252
 - ... *see also*: keying material, session keys (802.11)
 - key agreement 93–94
 - ... *see also*: DH, ElGamal, EKE, PAKE, SPEKE, STS
 - key continuity management 220, 241
 - key derivation function, *see*: KDF
 - key distribution 37
 - ... *see also*: key agreement, key establishment, public-key distribution
 - key distribution center, *see*: KDC
 - 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, *see*: KTC
 - 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
 - KeyID field, *see*: MAC frame (KeyID field)
 - keying material 93, **95**–97, 101, 104, 236, 252, 254
 - keyjacking 200
 - keylength 34
 - ... recommended 50
 - keylogger (keystroke logger) 18, 57, 78, **196**, 203, 207, 274
 - keyring, *see*: PGP
 - keystream
 - ... pseudo-random 354
 - ... recovery (WEP), *see*: WEP (keystream recovery)
 - ... reuse (WEP), *see*: WEP (keystream reuse)
 - ... *see also*: stream cipher
 - keystroke dynamics 87
 - Kismet, *see*: wireless analysis tools
 - knowledge-based authentication, *see*: what you know
 - known-key security 104
 - known-plaintext attack, *see*: attack models (ciphers)
 - KoreK, *see*: chop-chop attack
 - KTC (key translation center) 96
 - Kuang decision tree 27

L

Lamport hash chain 42, **67**–68, 86
 LAN (Local Area Network) 303, 311, **316**, 327–328, 331, 334, 340, *see also*: WLAN
 LAND (LAN denial, DoS attack) 321, 334
 Latin-1 (character encoding) 266
 law enforcement 196, 240
 layer 2 (802.11) 342–343, 364
 ... access control 347, 349
 ... association 342
 ... connection 342
 ... wireless link 350
 ... *see also*: link-layer
 LDAP (Lightweight Directory Access Protocol) 222, 229, 238, 254
 leap-of-faith (trust), *see*: TOFU
 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
 legality and ethics (wireless access) 345
 length-preserving 35
 Let's Encrypt (certificate service) 230, 270
 libc (C library) 167, 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
 link vs. end-to-end security (wireless) 343
 link-layer access control, *see*: layer 2 (802.11)
 link-layer protection 347
 linkability 378
 linked list 377
 linking and loading (linkers) 199
 Linux 126, 288
 ... kernel backdoor 196
 ... kernel module signing 208
 ... capabilities 175, 199
 ... security module (LSM) 145–146
 listing (directory), *see*: ls
 literal content (HTML, SQL) 266, 268
 liveness property 104, 366
 LKM (loadable kernel module) 199
 LLC/SNAP header (subnet access protocol) 359–360
 LLL (Ethereum programming language) 404
 ln (command), *see*: link
 load balancing 325–326
 loadable kernel module, *see*: LKM
 loader, *see*: linking and loading
 location (HTML, HTTP) 255
 Location (HTTP header) 255

lock icon (browser) 230–232, 270–272, 274
 lock-time (Bitcoin) 380–381, 383, 391
 locking script (Bitcoin) **380**, 384, 391
 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
 low-level authentication (802.11) 341–343, 347
 ls (list command) 138, 141
 lvtres (keylogger rootkit) 196

M

M-AC (mandatory access control) 144–146, 152
 MAC (message authentication code) **45**–48, 64, 254
 MAC address (media access control address) **303**, 316, 327–328, 341–345, 362–363
 ... allowlist, *see*: allowlist (MAC address)
 ... broadcast 342, 366
 ... multicast 342, 366
 ... randomization 370
 ... spoofing (falsely asserting) 344–346
 ... unicast 342
 ... used in nonce generation (802.11) 365
 ... used in PTK generation (802.11) 363
 ... used to bind session keys to devices 366
 MAC algorithms 361
 ... CBC-MAC 46–47, 361
 ... CMAC (AES-CMAC) 46, 48, 51
 ... HMAC 46, 48, 51, 274, 362, 367
 ... Poly1305 46–49, 51, 274
 MAC filtering, *see*: allowlist (MAC address)
 MAC flooding 328
 MAC frame (802.11) 341, 352
 ... body 341, 352
 ... format 341, 352–353
 ... header 341, 352
 ... IV for WEP, *see*: WEP (IV)
 ... KeyID field (frame body) 352, 362, 366
 ... nonce for CCMP CTR mode, *see*: AES-CCMP (nonce)
 ... PDU (protocol data unit), *see*: MPDU
 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
- management frames, *see*: frame types (802.11)
- mandatory access control, *see*: M-AC
- mangling rules (password guessing) 64
- manual gateway 289
- market for lemons 26–27
- Martian packets 323–324
- mashup (browser) 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
- master key (wireless, shared) 346, 358, 361
 - ... recovery, *see*: WEP (master key recovery)
 - ... static 357–358, 361
 - ... *see also*: PSK (802.11)
- matching score (classification) 73–74
- mathematical proof 17–18, 412
- Max-Age (cookie attribute) 256
- MDA (mail delivery agent) 235
- MD5 (hashing) 44, 51, 61–62, 274
- Mebroot (rootkit) 204
- media access control address, *see*: MAC address
- Melissa (virus) 189
- Meltdown (hardware side channel) 197, 413
- memory descriptor 127–128
- memory isolation 197, 199
 - ... *see also*: isolation
- memory layout 166–167
- memory pool, *see*: transaction (Bitcoin)
- memory protection 127–129, 197
- memory safety 163, 165, 172, 179
- mental model 22, 142, 246, 269–**270**, 273, 275, 289
- Merkle authentication tree (hash tree) 45, **384**–385, 406
- Merkle path authentication 386, 395
 - ... proof of inclusion (in Merkle hash tree) 395
- Merkle Patricia Tree, *see*: MPT
- Merkle root (Bitcoin) **384**–388, 391, 395, 397, 403
- mesh networks 370
- message authentication (data authentication), *see*: data origin authentication
- message authentication code, *see*: MAC
- 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
 - ... wireless, *see*: rogue AP
 - ... *see also*: HTTP (proxy), TLS (interception)
- middlebox 254, 261, 298
- min-entropy 83, 85
- minimize-secrets principle 22
- miner (Bitcoin) 379, 381, 383–384, **386**, 388
 - ... abandoning in-progress block 388, 391
 - ... miner vs. full node 394
- mining (Bitcoin) 206, 381, 386–**387**, 391
 - ... hardware 406
 - ... pool (group of miners) **394**, 398–399, 404
 - ... pseudocode 387
- mining (Ethereum) 401
 - ... mining pool 404
 - ... proof-of-stake model 406
- mining bound (Bitcoin) 385–387, **389**–392
 - ... recalibrating 389–390
- Mirai (botnet) 325
- misfeasance 332
- misuse detection (IDS) 332
- mixed content 274
- mkdir (command) 141
- MLS (multi-level security) 144, 151–152
- mobile device management 370
- mobile phone (authentication), *see*: two-factor, what you have
- mobile station (802.11), *see*: STA
- mod (modular arithmetic), *see*: congruence
 - ... modular exponentiation 38–39
 - ... modulus 38–39, 50, 108–109, **115**, 117
- mode bit, *see*: supervisor
- model checking 179
- model-reality gap 16–18, 412
- modem (modem pool) 370
- modes of operation (block cipher) 35–36, 361
 - ... CBC 35–36, 274
 - ... CFB 36
 - ... CTR 35–36, 47, 361–362
 - ... ECB 35–36
 - ... OFB 36
 - ... XTS 36
 - ... *see also*: authenticated encryption
- modification detection code 43
- modular design, *see*: design principles
- monitor mode (RFMON mode, wireless) 346
- monitoring system 311, 315–317, 332–333
 - ... monitoring tools (wireless) 345–346
- monolithic (vs. modular design) 131, 199
- Morris worm, *see*: Internet worm
- mother’s maiden name, *see*: secret questions

mouse patterns, *see*: biometric modalities
 move-countermove games 190, 269
 MPDU (MAC protocol data unit) 341, 352, 355, 361–362
 MPT (Merkle Patricia Tree) 399, 402, **403**–404, 406
 MSA (mail submission agent) 235
 MSCHAP, MSCHAPv2 (authentication) 369–370
 MSDU (MAC service data unit) 362
 MTA (mail transfer agent) 235
 MTU (max. transmission unit, Ethernet) 304, 357
 MUA (mail user agent) 235
 multi-level security, *see*: MLS
 multicast address 342
 Multics **126**, 133, 146, 148–152, 413
 ... *see also*: protection rings, segment (addressing)
 multiplicative group 115, 117
 mutable fields 300, 361
 mutation engine (malware) 191
 mutual authentication **93**–94, 100, 103, 106, 114, 223, 274

N

Nakamoto, Satoshi 405
 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
 Namecoin 405
 NAT (network address translation) 287, 303, 306
 National Vulnerability Database, *see*: NVD
 need-to-know (principle) 22
 Needham-Schroeder protocol 120
 Nessus (vulnerability scanner) 318–319
 Netcat (nc) 320
 Netfilter framework 288
 netstat (network statistics) 319
 NetStumbler (wireless active scanning) 345–346
 Network Flight Recorder (NFR) 332
 network interface card (NIC) 316
 ... wireless 346
 network layer 291, **300**, 303–305, 328
 network mapping 318
 network protocol stack, *see*: network stack
 network protocols 300, 303–306
 network security 282–306, 310–334
 network stack 292, 298, **300**, 303, 328, 349–350
 Network Time Protocol, *see*: NTP
 network traffic analyzer 319
 network worm, *see*: worm
 NFT (non-fungible token) 405
 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
 node (Bitcoin) 377, 394
 ... full node 391, 394
 ... light node 394–395, *see also*: SPV (client)
 ... peer node 377
 non-executable (stack, heap) 171–172
 non-fungible token, *see*: NFT
 non-repudiation **4**, 15, 39, 45–46, 216–217
 nonce 35, 48–49, **99**–100, 114, 252–253, 365
 ... *see also*: AES-CCMP (nonce), block header (Bitcoin, mining nonce), Ethereum (nonce)
 notary 217
 NTAPI (Native API) 198
 NTP (Network Time Protocol) 324, 365
 NUL byte (C language) 167, 173, 177–178
 NULL pointer (C language) 177
 null authentication (802.11), *see*: Open System authentication
 null encryption (IPsec) 303
 NVD (National Vulnerability Database) 208

O

obfuscation 191–192, 265, 268
 object (access control) 130–133, 145
 object (DOM), *see*: DOM
 object (file, binary) 199, 208
 object identifier, *see*: OID
 object tag (HTML) 259, 265
 oclHashcat (password cracker) 64
 OCSP (Online Certificate Status Protocol) 222–223, 241
 ... OCSP-stapling 222, 241
 OFB (Output Feedback Mode), *see*: modes of opn
 off-path (blind) attacks 332, 334
 offline password guessing 57–65, 77–78, 86, 92, 98, 105–106, **107**–111, 120, 217
 OID (object identifier) 230
 OKE (Open Key Exchange) 111
 ommer, *see*: block (Ethereum, uncle)
 on-path attacks 329–331, 334
 on-the-fly guessing attacks 60, 63–64
 one's complement (binary representation) 164
 one-time pad (stream cipher) 33, 51, 354, 356
 one-time password, *see*: OTP
 one-way property 41
 ... one-way hash function, *see*: hash function
 online password guessing 57–65, 78, 80, 84–86, **107**–108, 120, 161, 306, 319, 396
 opcode (machine code) 168, 170, 177, 195, 199
 open (system call) 157–159
 open AP (no encryption) 367–368
 open design, *see*: design principles
 Open System authentication (802.11) **342**–343, 349, 353

- OpenID 120
 - OpenPGP 239, 241
 - OpenSSH 293
 - OpenSSL 22, 38, 232, 234
 - OpenVMS 151
 - OpenVPN 303
 - operating characteristic, *see*: ROC
 - operating system, *see*: OS
 - operational practice (issuing certificates) 230, 241
 - opponent, *see*: adversary
 - opportunistic attacks 10
 - opportunistic encryption 21, 254
 - Opportunistic Wireless Encryption, *see*: OWE
 - OPRETURN (Bitcoin opcode) 383, 406
 - 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, *see*: OV certificate
 - origin, *see*: SOP (same-origin policy)
 - orphan pool, *see*: transaction (Bitcoin, orphan pool),
block (Bitcoin, orphan block pool)
 - OS (operating system) 151, 178
 - ... security **126**–152
 - ... fingerprinting 318, 333 (*re*: Nmap, p0f, Xprobe2)
 - OS/2 151
 - OSI stack, *see*: network stack
 - OTP (one-time password) 17, 23, **67**–70, 86, 99,
294, 329
 - out-of-order execution (side channel) 197, 413
 - out-of-band (OOB) **95**–96, 218–219, 237, 252, 306
 - ... *see also*: independent channel
 - outbound (packet) **283**–292, 333
 - output escaping, *see*: escape
 - outsider, *see*: insider/outsider
 - OV (Organization Validated) certificate **230**, 270, 272
 - OWASP 262, 269, 275
 - OWE (Opportunistic Wireless Encryption) 367–368
 - owner (file), *see*: user (file owner)
- P**
- p0f (OS fingerprinting) 318, 333
 - P2PK (Pay-to-Public-Key) 380, 384
 - P2PKH (Pay-to-Public-Key-Hash) 380, 383–384
 - P2SH (Pay-to-Script-Hash) 380, 383–384
 - packet (networking) 303–306, 311
 - packet filter, *see*: firewall
 - packet sniffing (capture utilities) 316, **319**, 332–333
 - padding 34, 301
 - page reloads 260
 - paging (memory) 136
 - pairwise master key (802.11), *see*: PMK
 - pairwise transient key (802.11), *see*: PTK
 - PAKE (password-authenticated key exchange) **105**–
111, 120, 273–274, 370
 - ... browser integration 273–274
 - PAP (authentication) 369–370
 - parasite (hosted malware) 207
 - parent (OS process) 137–138, 158, 175–176
 - parent block, *see*: block (Bitcoin, parent block)
 - parser (HTML, JavaScript, URI, CSS) 275
 - ... *see also*: HTML (parsing)
 - partial-guessing metrics (passwords) 85–87
 - 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, 396
 - passphrase 64, 69, 239, 295
 - passport analogy 218
 - passwd (command), *see*: /usr/bin/passwd
 - password (password authentication) 56–59, 129
 - ... advantages 59
 - ... attacks on password authentication **15**, 57–58, 78
 - ... attack defenses 60–65
 - ... capture 57–58
 - ... cracking tools 64
 - ... default 317
 - ... disadvantages 58
 - ... distribution (skewed) 63
 - ... interference 59
 - ... length 62
 - ... master 77, 113
 - ... NIST guidelines 64–65, 87
 - ... pro-active checking 63
 - ... recovery, *see*: account (recovery)
 - ... recovery (Bitcoin) 396
 - ... reuse 58, 68, 72
 - ... stored hash 57
 - ... synchronization 77
 - ... system-assigned 61, 86
 - ... usability 58–59, 62, 64–65, 77
 - ... user-chosen 63, 396
 - ... user-chosen (WEP) 351, 358–359
 - ... 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
 - ... guesswork, *see*: guessing function
 - ... SSH password guessing 306
 - ... *see also*: Bitcoin (password risks), password (user-
chosen, WEP)
 - 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, *see also*: zxcvbn
- password portfolios 87
- password reset 65–66, 86
- password sniffing, *see*: password (capture)
- password stretching 60
- password-authenticated key exchange, *see*: PAKE
- PasswordMultiplier (password manager) 78
- patching (software update), *see*: update
- Path (cookie attribute) 256, 259
- path (pathname, filepath) 177, 247, 256, 258, 263
- path authentication, *see*: Merkle path authentication
- path of least resistance 23
- path-access (filesystem) 139, 259
- path-based permissions, *see*: path-access
- pathLenConstraint (extension) 221, 228
- pathname resolution 143, 157–159, 178, 197
- Patricia tree (compressed trie) 403–404, 406
- PaX project (Linux) 179
- pay-per-install 208
- payload 38, 47, 187, 196, 283, 317
 - ... HTTP 251, 288
 - ... IPsec 301–302
 - ... TCP 304
- payload length (physical layer) 341
- PCA (Policy Certification Authority; PEM PCA) 329
- pcap (packet capture) 319
- PDU (MAC protocol data unit), *see*: MPDU
- PEAP (Protected EAP) 369
- peer-to-peer network 45, 379, 386
- 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 (URI characters) 266
- perfect forward secrecy, *see*: forward secrecy
- perimeter defense 17, 282–283, 285–287, 291, 318, 347
 - ... *see also*: firewall
- Perl (language) 264
- permission bits (filesystem) 128, 132
- permissions 128
 - ... (user, group, other) model, *see*: ugo
 - ... on directories 138–139
 - ... on files 133
 - ... RWX 128, 132, 135–136, **138**–139, 141, 148
- permutation 35, 193
- persistent state (in browser plugins) 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, 411
 - ... and certificates 270
 - ... defenses 271
 - ... enablers 270, 275
 - ... spear phishing 270
 - ... transient phishing site 271
- Photuris protocol (DH variant) 323
- PHP (language) 264
- physical address (LAN) 303
- physical address space 199
- physical interface (switch port) 328
- physical layer 341
- Physical Layer Convergence Protocol, *see*: PLCP
- PID (process identifier) 129, 137, 150, 319
- 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, 214–15, **216**–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
- plaintext recovery (if Vernam keystream reused) 369
- PLCP (Physical Layer Convergence Protocol) 341
- PMF (protected management frames, 802.11) 346, 365, 368
- PMK (pairwise master key, 802.11) **348**–350, 363, 365–367
- PN, *see*: AES-CCMP (packet number)
- Pohlig-Hellman algorithm 117
- pointer arithmetic (C language) 162, 165, 173
- pointer protection 173
- poison packets 321, 325, 331
- policy (security) **4**–6, 18–19, 62, 282–284, 310, 318
 - ... access control 130–131
 - ... access point (AP) 343
 - ... 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 284, 286
- ... IPsec 303, 306
- ... operational (certification authority) 216
- ... policies for plugins 259
- ... remote access policy 5
- ... violation of security policy 5
- ... WLAN policy 364
- ... *see also*: password expiration, password composition
- Policy Certification Authority (PEM), *see*: PCA
- policy script component (IDS) 315
- policy-based packet filtering (IPsec) 303
- Poly1305, *see*: MAC algorithms
- polyalphabetic substitution 51
- polymorphic virus, *see*: virus
- Ponzi scheme 405
- POP3 (email retrieval) 235, 254, 304
- port (TCP, UDP) 175, 247, 258, 283–288, 295, 303, 304–305, 318
- port (802.11)
 - ... controlled port 348
 - ... uncontrolled port 348
 - ... *see also*: IEEE 802.1X
- port forwarding (SSH) 295–296
- port mirror 316
- port scanning, *see*: scanning (TCP, UDP ports)
- port stealing 328
- positive validation 269
- POST (HTTP request method) 249, 261–262, 274
- postfix expression (notation) 382
- postMessage 274
- postprocessing results (inline hooking) 198
- PPP (Point-to-Point Protocol) 369–370
- pre-capture attack, *see*: attack
- pre-shared key, *see*: PSK
- preimage 42
 - ... preimage resistance 41–42
- prepared statements (SQL) 269
- preview panes (email auto-preview) 205
- PRF (pseudo-random function) 362–363, 365
 - ... for deriving sequences of keys (Bitcoin) 398
 - ... *see also*: AES-CCMP (key hierarchy), KDF, PRNG
- 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, 368, 370
- 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
- PRNG (pseudo-random number generator) 120
 - ... *see also*: PRF, RNG
- proactive password cracking 63, 317
- probabilistic encryption, *see*: ElGamal encryption
- probability distribution 74, 82, 85
- probability of guessing success 62
- probable prime number 333
- probe (802.11) 341, 342–343, 345–346
- probe (scan) 318, 333
- process creation 175–176
- process identifier, *see*: PID
- processes (operating system) 149–151
- profile (IDS) 314–315, 332
- Program Counter (PC), *see*: Instruction Pointer
- promiscuous mode
 - ... wired network 316, 319
 - ... wireless 346
- proof by contradiction 190, 208
- proof of knowledge 68, 97, 103, 112, 216, 229, 253
 - ... *see also*: challenge-response
- proof of work 381, 389, 391–393, 395
 - ... greatest aggregate proof of work 392
- proof-of-stake model, *see*: mining (Ethereum)
- protected management frames (802.11), *see*: PMF
- protection (operating system) 126
- protection bit initial values 135, 141
- protection domain 129–130, 149–151, 257
- protection group, *see*: group
- protection rings (access control, Multics) 146–152
 - ... access bracket 147–150
 - ... brackets (read, write, execute) 148
 - ... ring number 147, 150
- protocol 92
- protocol data unit, *see*: PDU
- protocol scrubber 333
- provably secure 4
- proxy (firewall), *see*: firewall (proxy)
- proxy server, *see*: HTTP (proxy server)
- proxy-aware client 288–289
- proxy-aware gateway 288
- pseudo-protocol (HTML) 248

- pseudo-random bit generation, *see*: PRF
 pseudo-random number generator, *see*: PRNG
 pseudonym 216, 378
 PSK (pre-shared key, TLS) 252–253
 PSK (pre-shared key, 802.11) **348**, 350, 359, 363–365, 368
 ... derived from SSID and password 367
 ... password-to-PSK mapping 367
 ... shared among users 367, *see also*: master key
 ... shared and public 367–368
 psychological acceptability 273
 PTK (pairwise transient key, 802.11) **363**, 365–367
 PTW attack (WEP) 360
 public key pinning 241
 public-key algorithms, *see*: DH, EC, ElGamal, 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 authentication 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
 puzzle (Bitcoin) 386
 ... *see also*: mining bound (Bitcoin)
 PwdHash (password manager) 78
 Python (language) 162
- ## Q
- query data (HTTP) 247, 250
- ## R
- RA (Registration Authority) 217
 rabbit (malware) 205, 321
 race conditions (access control) 152, **157–159**, 175, 178
 ... *see also*: TOCTOU
 radio frequency, *see*: RF
 radio jamming, *see*: DoS (radio jamming)
 RADIUS (Remote Authentication Dial In User Service) 347–**350**, 369–370
 ... server 341, 370
 ... support for EAP 369
 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, *see*: RNG
 random variable 82
 randomization of ephemeral ports 334
 randomized encryption 101
 ransomware 186, 196, **202–203**, 206–208
 ... incidents 203
 RAT (remote access trojan) 195
 rate limiting (throttling) 59, 63–64, 86, 161, 325
 raw sockets 322
 RBAC (role-based access control) 144–145, 151
 RC4 49, 51, 274, **351**
 ... key setup in WEP 351, 359
 ... seed key in WEP 351–352, 357, 359
 ... use in WEP **351–352**, 364–365
 ... weak IVs (initial keystream bytes) 359–360
 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
 reconnaissance (wireless) 345
 recursive query (DNS) 326
 redirection (HTTP response) 252
 redirection (web) 200–201, 246, **251–252**, 255, 263–265, 269
 reduction modulo 2^n 162, 165
 redundancy function (within digital signature) 51
 reference integrity, *see*: request-response integrity
 reference monitor **130–132**, 152
 reference validation mechanism 131
 REFERER header (HTTP) 249–250
 reflection attack, *see*: attack
 reflectors (networking, DoS) 333
 Refresh header (HTTP response) 251
 refresh meta-tag (HTML) 251
 Registration Authority, *see*: RA
 regular expression 314
 relational database 266
 relative addressing 177–178, 188, 199
 relay attack, *see*: attack
 relocation (machine code) 199
 reluctant allocation, *see*: design principles
 relying party 49, 113, **215**, 221–222, 224, 229, 236
 remnant removal, *see*: design principles
 remote access trojan, *see*: RAT
 remote administration (remote desktop) 195
 ... remote desktop tools 195
 remote OS fingerprinting, *see*: OS (fingerprinting)
 remote shell 293
 remote-access commands 292–293
 replay attack, *see*: attack
 replay protection
 ... IPsec 300–302
 ... TLS 254
 ... *see also*: AES-CCMP, transaction (Ethereum)
 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 (attack) 171–172, 179
 - reverse engineering 185, 191–192, 204, 208
 - reverse Turing test, *see*: ATT
 - revocation, *see*: certificate revocation
 - rexec (remote execution) 194, 292
 - RF (radio frequency) 340
 - ... ranges 340
 - RFC (Request For Comments, IETF) 224, 369
 - ... standards-track 369
 - RFMON mode, *see*: monitor mode (wireless)
 - .rhosts file 296–297
 - Rijndael (AES) 34
 - ring (access control), *see*: protection rings
 - RIPEMD160 (hashing) 378, 397, 406
 - risk 6, 78
 - ... assessment 6–9, 27
 - ... equation 6–7
 - ... management 9
 - ... rating matrix 9
 - ... wireless 347
 - RISOS report (1976) 152
 - rlogin (remote login) 194, 291–293, 297
 - RNG (random number generator) 95, 120
 - ... *see also*: PRNG
 - robust network 364, *see also*: RSN
 - ROC (receiver operator characteristic) 74–75, 87
 - rogue AP (wireless middle-person) 342, 344, 346–347, 366, 368–369
 - ... *see also*: DoS (via rogue AP)
 - role (access control) 129, 144–145
 - ... role-based access control, *see*: RBAC
 - root (UNIX) 134, 156
 - ... of filesystem 140
 - ... root privilege (UID 0) 134, 198
 - ... UID 0 vs. kernel 175
 - root CA (certification authority) 225–228
 - root of trust, *see*: trust anchor
 - root shell 175–176, 192
 - rooted (compromised) 195
 - rootkit 156, 189, 192–194, **195**–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 350
 - routing-based attacks 334
 - RSA (Rivest Shamir Adleman algorithm) **38**–39, 41, 50–51, 69, 100, 108, 121, 203, 253, 274, 306
 - rsh (remote shell) 194, 292–293, 297
 - RSN (robust security network 802.11) 365, **367**, 370
 - RSNA (RSN association) 367
 - RST (reset, TCP) 283, **304**, 311, 322, 330–332
- ## S
- S/KEY 86
 - S/MIME 220, 224, 235, **238**–239, 241
 - SA (security association) 348
 - ... IPsec SA 300–301
 - SAE (Simultaneous Authentication of Equals) 365, 368, 370
 - 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, *see*: SOP
 - same-ports strategy 254, 274
 - sandbox 21, 151, 174–175
 - sanitization, *see*: input sanitization
 - SATAN (audit tool) 319, 333
 - satoshi (subunit of BTC) **381**, 388
 - scan detection (IDS) 318, 333
 - scanning (TCP, UDP ports) 192, 318–320, 333
 - ... context-aware 192–193
 - ... hit-list 193
 - ... Internet-scale 193
 - ... localized 192
 - ... permutation 193
 - ... stealthy 333
 - ... topologically-aware 193
 - ... *see also*: reconnaissance
 - scanning (wireless, active) 345
 - scheme (URI access protocol) 247, 258
 - Schnorr signature scheme 121
 - scp (secure copy) 293, 296–297
 - screening router **287**, 291–292, 320
 - script (Bitcoin) 382, 400
 - ... execution example 382–383
 - ... redeem script 384
 - ... scriptPubKey 380, 382
 - ... scriptSig 380–382
 - ... semantics 380

- ... validation 383, 386
- ... *see also*: locking script, unlocking script
- script tag (HTML) 248, 257, 263
- scripting languages 200, 248
- script (hashing) 61
- SEAndroid (security-enhanced Android) 145–146
- search (command), *see*: find
- search tree 403–404
- second-preimage resistant 42
- secp256k1 (ECDSA curve), *see*: ECDSA
- secret prefix (hashing) 46
- ... secret suffix 46
- ... secret envelope 46
- secret questions 65–66, 86
- ... *see also*: account (recovery)
- secret validation tokens (CSRF) 262
- secret-key cryptography, *see*: symmetric crypto
- Secure (cookie attribute) 256, 259, 261
- secure 4–5, 18–20, 33
- secure attention sequence, *see*: trusted path
- secure composition 412
- 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 413
- security
 - ... analysis (process) 9–11, 17–19
 - ... by design, *see*: design principles
 - ... by obscurity 21
 - ... cues, *see*: security indicators
 - ... kernel 131, 151–152
 - ... label 145
 - ... mechanisms 6, 18–19
 - ... metrics 27, 62, 75, 85–86, 312–313
 - ... model 11, 18, 260, 412
 - ... model limitations 412
 - ... policy, *see*: policy
 - ... questions, *see*: secret questions
 - ... requirements 5, 11, 18–20, 65, 75, 104, 126, 131, 412
- security association, *see*: SA
- security clearance, *see*: classification level
- security indicators (cues) 26, 246, 270–275, 411
- ... negative indicators 272
- Security Parameters Index (IPsec), *see*: SPI
- security policy database (IPsec) 303
- security tunnel, *see*: tunnel (encrypted)
- SecurityFocus (vulnerability database) 208
- segment (addressing) **128**–129, 146–147
 - ... descriptor register **127**–128, 149
 - ... descriptor segment **128**–129, 149–150
 - ... segment descriptor **128**–129, 133, 146–150
 - ... segmented addressing 126, 146, 152
- segment (TCP) 300, 304, 329–331
- SegWit (segregated witness, Bitcoin) 379, 406
- 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 (TVP) 99
 - ... IPsec 300, 302
 - ... TCP 300–302, 305, 322, 324, 329–**330**
- sequences of system calls 311, 315
- server certificate, *see*: TLS (certificate)
- Server Name Indication, *see*: SNI
- service set identifier, *see*: SSID
- session creep (IDS) 315
- session hijacking, *see*: hijacking
- session ID (HTTP) 260, 294
- session key, *see*: key
- session keys (802.11) 348, 365
 - ... liveness 366
 - ... *see also*: AES-CCMP, PTK
- 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) 413
- SHA (Secure Hashing Algorithm) **44**
 - ... SHA-1 **44**, 61, 232, 274
 - ... SHA-2 (SHA-256, SHA-512) **44**, 232, 274
 - ... SHA-3 **44**, 274, 399, 406
 - ... SHA256 **44**, 378, 387, 391, 397, 404, 406
- shadow password file, *see*: /etc/shadow
- shadow stack 173
- Shannon entropy, *see*: entropy
- Shared Key authentication (802.11) 342, **353**, 356, 358, 367
- shell (command interpreter) **176**–178, 188, 203, 293
 - ... shell script 188
- shellcode 156, 170–172, 175 **176**–179, 203
- short exponents 50, 119
- shoulder surfing (password capture) 57
- side channels 15, 23, 197, 370, 413
- 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*: IDS
- signed code, *see*: code signing
- signed integer, *see*: two's complement
- signedness error (sign conversion), *see*: integer vulnerabilities
- SIM swap attack (subscriber identity module) 67
- Simple Mail Transfer Protocol, *see*: SMTP
- simple payment verification, *see*: SPV
- simplicity and necessity, *see*: design principles
- single-credential system 113
- single point of failure 23, 78, 204
- single sign-on, *see*: SSO
- small trusted bases, *see*: design principles
- small-subgroup attack 101–102, 110, 118, 115–121
- smart contract 376, 399, 405–406
 - ... categories (use cases) 405
 - ... examples 406
 - ... programming pitfalls and attacks 406
 - ... security analysis and tools 406
- SMS (Short Message Service) 66–67, 86–87, 240
- SMTP (Simple Mail Transfer Protocol) 229, 235, 254, 284–285, 304
- Smurf attack (flood) 323, 325, 334
 - ... mitigation 323
- SNI (Server Name Indication) 241
- sniffing (wireless) 346
- Snort (IDS) 315, 319, 332–333
 - ... snort2bro 315
- social engineering 26, 57, 67, 185, 187, 199, 202, 205–207, 261, 264, 270–271, 273, 411
- socket (IP) 284–285, 289–290, 304, 322, 330–331, 333
- SOCKS 289–290, 306
 - ... sockd (SOCKS daemon) 289–290
- software fault injection 333
- software installation 56, 185, 195, 205, 207
- software interrupt 164, 176
- software security 19, 156–178, 319
- software update 24, 413, *see also*: update
- SolarWinds (company, incident) 413
- Solidity (Ethereum programming language) 404
- Sony rootkit 196
- SOP (same-origin policy) 257
 - ... DOM SOP 246, 257–260, 274–275
 - ... matching origin 259
 - ... origin (definition) 257–258
 - ... origin server 255–257, 260
 - ... origin triplet 257–258
 - ... SOP for cookies 259, 274–275
 - ... SOP for plugins 259, 274
- source address spoofing, *see*: IP address (spoofing)
- SP (Stack Pointer) 167
- 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 (spam zombie) 207
- SPAN port (switched port analyzer) 316–317
- special protection bits 135–136
- specification-based IDS, *see*: IDS
- Spectre (hardware side channel) 413
- speculative execution (side channel) 197, 413
- SPEKE (simple password exponential key exchange) 94, 110, 120, 368
- SPI (Security Parameters Index, IPsec) 300–301
- spoofing 15, 76, *see also*: ARP spoofing, DNS (spoofing), IP address (spoofing), MAC address (spoofing), SSID (spoofing)
- SPV (simple payment verification) 395–396, 405
 - ... client (thin client) 395
 - ... confirmation 395
- 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
 - ... *see also*: dispatch table
- SSH (secure shell protocol suite) 185, 220, 241, 250–251, 258, 290, 292–298, 300, 306
 - ... channel 293–294
 - ... client authentication 294
 - ... connection protocol 293
 - ... host key 294, 306
 - ... host-based client authentication 296
 - ... multiplexed channel 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
- SSID (service set identifier) 342, 344, 346, 367
 - ... spoofing 342
- SSL (Secure Sockets Layer), *see*: TLS
- SSO (single sign-on) 113–114, 120
- STA (mobile station, 802.11) 340–341
- Stacheldraht (TFN-based DoS) 325
- stack frame 167–168
- Stack Pointer, *see*: SP
- stack querying (OS fingerprinting) 318, 333
- stakeholders 26, 240
- standard input/output streams, *see*: stdin
- stack-based computation 382

- startup file 139
 - stat (system call) 159
 - stateful packet filter 284
 - stateful protocol analysis 332
 - ... *see also*: IDS (specification-based)
 - stateless packet filter 284
 - stateless protocol (HTTP) 255
 - static analysis 173, 179, 269, 333
 - statically allocated variables 167
 - STARTTLS 254
 - Station-to-Station key agreement, *see*: STS
 - 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
 - storing passwords, *see*: password file
 - strep (C library function) 167, 171–173
 - stream cipher 32–34, 36
 - ... stream vs. block cipher 36
 - ... Vernam cipher **32–34**, 351, 354, 369
 - ... *see also*: ChaCha20, one-time pad, RC4
 - STRIDE (threat modeling) 12, 15–16
 - string (NUL-terminated, C) 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 (Station-to-Station) key agreement 94, **103**, 105, 120
 - 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
 - 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, 413
 - 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 flood (attack) 321–323, 325, 334
 - ... mitigation 323, 334
 - SYN packet (flag) **304**, 321–322, 329
 - ... SYN cache 323
 - ... SYN cookie 323
 - 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, *see*: SSDT
 - system specification 412
- ## T
- t-bit (filesystem), *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, **304–306**
 - ... 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, 412
 - ... *see also*: fuzz testing, penetration testing
 - TEthernet, *see*: Wireshark
 - text bit (filesystem), *see*: sticky bit
 - text message, *see*: SMS
 - TFN, TFN2K (Tribal Flood Network) 325, 334
 - 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
 - ... wired network 346
 - ... WLAN, *see*: WLAN (threat model)

- 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 (access control), *see*: access control (ticket)
- ticket (Kerberos) 114, 294
- time bomb (malware) 204
- time-memory tradeoff 86, 107
- time-of-check time-of-use, *see*: TOCTOU
- time-tested tools, *see*: design principles
- time-variant parameter, *see*: TVP
- timestamp (TVP) 99
 - ... *see also*: block (Ethereum, timestamp)
 - ... *and*: block header (Bitcoin, timestamp)
- timing attack (SSH) 306
- TK (temporal key), *see*: AES-CCMP (TK)
- TKIP (temporal key integrity protocol, 802.11) **364**–365, 367–368
- TLD (top-level domain) 247
- TLS (Transport Layer Security) 51, 229, 238, 241, 251, **252**–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
 - ... SSL history 241, 274
 - ... tunnel method for EAP, *see*: PEAP
- TLS-over-EAP 350
- TLS-SRP 273–274
- TLS-stripping attack 233, 241
- TOCTOU (time-of-check time-of-use) **157**–159, 178
- TOFU (trust on first use) **220**, 231, 241, 294, 306
- 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
- transaction (Bitcoin) 376–377
 - ... coinbase, *see*: coinbase transaction
 - ... confirmation, *see*: block (Bitcoin, confirmed)
 - ... example 380, 382–383
 - ... fees 381, 388, 406
 - ... ID, *see*: txID
 - ... inputs becoming outputs 379
 - ... length 385
 - ... list 385
 - ... malleability 397
 - ... memory pool 386–387, **388**–389, 391, 394
 - ... orphan pool (transactions) 389
 - ... orphan transaction 389
 - ... output, *see*: TXO
 - ... priority 388
 - ... provably unspendable 383
 - ... regular, *see*: Bitcoin (system, regular transaction)
 - ... unspendable 383
 - ... validation checks 391
 - ... validity 379, 382
- transaction (Ethereum) 399–401
 - ... fees 401
 - ... fields 400
 - ... receipt 401, 403
 - ... replay protection 401
 - ... sender's signature 401
 - ... up-front cost 401, 403
 - ... validation and execution 403
 - ... *see also*: gas (Ethereum)
- transport mode (IPsec) 299, 301–302
- transposition cipher 51
- trawling 57, 60
- tree authentication, *see*: Merkle authentication tree
- Tribal Flood Network, *see*: TFN
- trie (prefix tree) 404
- trinoo (DDoS) 325, 334
- triple-DES (3DES) 49–51, 274
- Tripwire (file change detection) 43, 190
- Trojan horse (malware) 152, 186, **194**, 196, 207
 - ... *see also*: Thompson's Trojan compiler
- true negative (TN) 312
 - ... true negative rate (TNR) 312–313
- true positive (TP) 312
 - ... true positive rate (TPR) 312
- trust agility 24, 234
- trust anchor (PKI) 24, 217–218, **219**–220, 223–230, 232–234, 237–239, 254, 377
 - ... list 227, 229
- trust anchor justification 220,
 - ... *see also*: design principles
- 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, *see*: TOFU
- trust sink 377
- trusted 4

- ... certificate 229
 - ... certificate store 219, 223, 254
 - ... computing 214
 - ... login hosts 297
 - ... server 96, 113, 222–223, 237
 - ... transitive trust 23, 221, 234, 297
 - ... trusted vs. trustworthy 4
 - trusted path (input/output) 71–72, 267, 273, 275
 - trusted third party, *see*: TTP
 - ... *see also*: CA, identity provider, KDC, KTC, RA
 - trustworthy **4**, 27, 224, 251
 - TTL field (time-to-live) 300–301, **305**–306, 326
 - TTP (trusted third party) 113, 215
 - tunnel (encrypted) 250–251, 253, 282, 286, 290, 292–293, 297, **298**–300, 303, 306
 - tunnel mode (IPsec) 299, 301–302
 - tunneling (protocol) 250, 286, 288, 295, **298**, 302
 - tunneling a port 295
 - Turing completeness 400
 - TVP (time-variant parameter) 68, 99, *see also*: nonce, random number, sequence number, timestamp
 - two-factor authentication (2FA) 67–70, 86, 287
 - two-stage authentication 70, 72
 - two's complement (binary representation) 160–166, 178
 - txID (transaction ID, Bitcoin) 380
 - TXO (transaction output, Bitcoin) 378
 - type casting (C language) 160–163, 173
 - type conversion 159–163
 - type promotion 160–163
 - type safety (type-safe language) 160, 170, 173
 - typing rhythm, *see*: biometric modalities
 - typosquatting 270
- U**
- UDP (User Datagram Protocol) 283, 285, 290, 300, **304**–306, 326, 334, 350
 - ... amplification 324
 - ... flood 323, 325, 334
 - ... packet forwarding 290
 - UID (user ID) **129**, 134, 137, 150, 157
 - ... effective UID (eUID) 137
 - ... real UID, saved UID (rUID, sUID) 137
 - ... UID 0 vs. kernel 175
 - ugo (user, group, other) permission model 134, 136
 - umask (protection bits) 135–136
 - unauthenticated key establishment 93–**94**, 102–104, 109, 367
 - undecidable problem 189, 208
 - underground economy 208
 - unicast address 342
 - Unicode, *see*: character encoding
 - uniform resource identifier, *see*: URI
 - uniform resource locator, *see*: URL
 - unilateral authentication 93–94, 112, 223
 - Unix **126**, 131, 133, 151, 167, 176–177, 188, 198, 207, 292–293, 297, 327, 333
 - ... security 207
 - ... time 385
 - ... viruses 208
 - unknown key-share attacks 120
 - unlink (system call) 158
 - unlocking script (Bitcoin) **380**–381, 384, 391, 406
 - unmotivated user 273
 - unqualified name 247
 - unsigned integer (C language) 161–166
 - unspent transaction output, *see*: UTXO
 - untraceability 377
 - update **24**, 186, 194–195, 204, 216–217, 314, 317–318, 325, 413
 - upper-layer authentication (802.11) 341, 343–345, 347–348, **368**
 - ... mutual 344–345, 347, 361, 365, 367–369
 - ... unilateral 344
 - URI (uniform resource identifier) **247**, 249–252, 256–259, 265–266, 275
 - ... reserved characters 266
 - URL (uniform resource locator) **246**–252, 255, 258, 263, 270
 - ... syntax 247
 - ... 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, 411–412
 - ... design principles 273
 - ... evaluation methods 412
 - ... user compliance 23, 26
 - use-after-free (memory) 179
 - user (file owner) 134–136
 - user acceptance, *see*: user buy-in
 - user agent (HTTP) 249
 - user authentication 56–87
 - ... categories 70
 - user buy-in 23, 75, 240, 273,
 - ... *see also*: design principles
 - (user, group, other) permission model, *see*: ugo
 - user ID (OS), *see*: UID
 - 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) 412
 - user workflow 12
 - userid (user ID), *see*: UID, username
 - username (account name) 56, 129
 - /usr/bin/passwd (password command) 137, 176
 - UTF-8, UTF-16, UTF-32 (character encoding) 265–266
 - UTXO (unspent transaction output, Bitcoin) **378**, 383, 388, 391, 396
 - UTXO pool (Bitcoin) 394

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 (Vernam)
 version detection 318
 virtual circuit 289
 virtual machines (and malware) 208
 virtual memory address 126, 128, 149, 152
 virtual private network, *see*: VPN
 virtual table (vtable), *see*: dispatch table
 virtual terminal connection, *see*: telnet
 virus 185, **186**–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 (virtual private network) 224, 282, 287, 297, **298**–303, 306
 ... architecture 299
 ... designs 299
 ... use cases 299
 vulnerability 5, 320
 ... assessment 11, 27, 179, 311, **317**–318, 333
 ... scanners 317–320, 333
 Vyper (Ethereum programming language) 404

W

wallet (Bitcoin) 379, 388, 395, **397**–398, 406
 ... client vs. cloud wallet 397
 ... hierarchical deterministic (HD) 396–398, 406
 ... hot vs. cold storage 397
 ... key management 406
 ... paper vs. hardware wallet 397
 ... use of 2D barcodes 397
 WannaCry (ransomware) 202–203, 208
 war driving 345–347, 369
 wardialing 345
 Ware report (1970) 152
 watch-only wallet (Bitcoin) 398, 406

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, **249**–250, 261–262, 264, 267
 ... hidden form 262
 ...submit button 249
 web hosting (site hosting) 234
 web of trust, *see*: PGP
 web origin, *see*: SOP (origin)
 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
 wei (subunit of ETH) 399–401
 weird machine 413
 WEP (wired equivalent privacy) **350**–353, 364, 369
 ... access control failure 356
 ... and RC4, *see*: RC4
 ... and WPA3 368
 ... attacks on 353, 360, 363
 ... ciphertext data (computation of) 355
 ... data integrity mechanism 356, *see also*: ICV
 ... excluded from RSN 367
 ... frame format 352–353
 ... ICV (integrity check value) 352–355
 ... ICV failure 353–356, 358
 ... IV (initialization vector) 352, 356–357
 ... IV (24-bit, too short) 356, 358
 ... IV collision 356–358
 ... IV reuse 354, 357, 364
 ... key management, *see*: IEEE 802.11
 ... KeyID field, *see*: MAC frame (KeyID field)
 ... keystream dictionary 357
 ... keystream recovery 353–354
 ... keystream reuse **354**, 356, 358, 364, 369
 ... keystream stripping 353
 ... master key recovery 357–360
 ... recap of problems 364
 ... security design properties 357
 ... timeline 364–365
 ... user-chosen password, *see*: password (user-chosen)
 WEP bit 353, **367**
 WEPCrack, *see*: wireless analysis tools
 WFA (Wi-Fi Alliance) 364, 368
 ... Easy Connect 368
 ... Enhanced Open 368
 ... specifications 365, 369
 ... WPA, *see*: WPA, WPA2, WPA3

... Wi-Fi Protected Setup, *see*: WPS
 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*: allowlist
 why security is hard **25–27**, 120, 411
 Wi-Fi (IEEE 802.11) 13, 300, 327, **340**
 ... hotspot (access point) 346
 ... passwords in coffee shops 367
 Wi-Fi 4 (Wi-Fi 5, Wi-Fi 6) 365
 Wi-Fi Alliance, *see*: WFA
 Wi-Fi Protected Access, *see*: WPA
 Wi-Fi Protected Setup, *see*: WPS
 widget (web) 201
 wildcard domain 230
 window object (DOM) 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, *see*: AP
 ... risks, *see*: WLAN (threats)
 ... in hotels, coffee shops 250, 287, 327
 wireless analysis tools
 ... Aircrack, Aircrack-ng 346, 360
 ... AirSnort 345, 360
 ... Kismet 346
 ... WEPCrack 360
 wireless DoS, *see*: DoS (wireless)
 wireless local area network, *see*: WLAN
 Wireshark (Ethereal) 319
 WLAN (wireless local area network) 340–341
 ... architecture 340
 ... in-range of service 341–342, 345–347
 ... infrastructure mode (802.11) 341–342
 ... security **340–373**
 ... security architecture 347
 ... threats and mitigations 287, 297, 327, 343, **347**
 ... threat model (physical basis for) 347
 ... *see also*: attack (wireless)
 work factor 23
 working key, *see*: key
 world-writable file 139–140, 158
 worm 185, **186–187**, 190–194, 207
 ... flash worm 193, 208
 ... incidents 191, 193–194
 ... self-stopping 190

... spreading techniques 187, 191–194, 201, 208
 WPA (Wi-Fi Protected Access) 350, **364–365**, 369
 WPA2 **364–365**, 368–369
 ... WPA2-Personal 368
 ... formal analysis 370
 WPA3 344, 364–365, **368**
 ... compliance 369
 ... transition mode (WPA2 interoperability) 368
 ... WPA3-Enterprise 365, 368
 ... WPA3-Personal 365, 368
 WPS (Wi-Fi Protected Setup) 368
 wrap around (integer) 161–162, 165
 wrapper function 176–177, 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
 XEX (XOR Encrypt XOR), *see*: XTS
 XMLHttpRequest 260, 275
 XMPP (Extensible Messaging and Presence Protocol) 254
 XOR (exclusive-OR) 33–35
 Xprobe2 (OS fingerprinting) 318, 333
 XSS (cross-site scripting) **262–266**, 274–275
 ... defenses 264–265, 275
 ... DOM-based XSS 263
 ... reflected XSS (non-persistent) 263–264
 ... stored XSS (persistent) 262–264
 XTS (XEX Tweakable Block Cipher with Cipher-text Stealing), *see*: modes of operation

Y

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

Z

Zeek (Bro, IDS) **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
 .zip file (compression) 206
 ZMap (Internet scanning tool) 333
 zombie (compromised) 201, **203–204**, 207, 321
 zxcvbn (password meter) 87