INDEX

A

access control, 199–221
  case study, 207–210
  violations, 225
access-control lists (ACLs), 207
active protection measures, 191
Advanced Encryption Standard (AES), 30, 95, 172
  `AddRoundKey()`, 30–32
  AES-CBC, 33, 37, 77, 95, 127, 134
  AES-CBC-ESSIV, 96
  AES-CMAC, 37
    RFC 4493, 37
  AES-CTR, 34, 76
  AES-GCM, 38, 77, 123, 126, 136
  AES New Instructions, 70, 74
  Canright S-box, 73
  crypto implementations, 73
  key expansion, 73
  `MixColumns()`, 30–32, 74
  operations, 31
  Rijndael, 30
  `ShiftRows()`, 30–32, 74
  state, 30
  `SubBytes()`, 30–32, 74
  T-tables, 74
Advanced High-performance Bus (AHB), 58
AEAD. *See* authenticated encryption with associated data
AES. *See* Advanced Encryption Standard
air gap, 121
AIS-32, 58
AMD, 91
Amnesia:33, xxii
Android, 19, 88, 156, 212
  seamless system update, 167
  verified boot, 144
anti-debugging measures, 92, 156
Apache, 216, 236
AppArmor, 232
  `aa-complain`, 218
  `aa-disable`, 216
  `aa-enforce`, 216, 220
  `aa-status`, 215–217
  case study, 214–221
  complexity, 214
  custom profile, 218, 220
  /etc/apparmor.d/, 216
  modes, 213, 218
  paths, 213
  profiles, 213, 216
  profiling, 218
application-specific integrated circuit (ASIC), 93
apps. *See* software applications
Argon2, 93, 94–96
ARM Boot Loader stage 2 (BL2), 150–152
ARM Cortex-A7, 76, 149, 192
ARM Cortex-M4, 149–150, 192, 196
ARM Product Security Architecture (PSA), 16
ARM Trusted Firmware, 142
ARM Trusted Firmware-A (TF-A), 150–152
ARM TrustZone, 142, 150–151, 240
asymmetric cryptography, 40–41, 45, 48, 74–75
asymmetric multiprocessing (AMP), 188
attackers
  cybercriminals, 11, 143, 200
  insiders, 12
  nation-state attackers, 12
  physical attackers, 13, 87
  product pirates, 12, 86
  script kiddies, 11
  security researchers, 11

attacks
- backdoor, 227
- brute-force, 28, 93, 235
- code lifting, 87, 92
- Compression Ratio Info-Leak Made Easy, 127
- crafted updates, 161
- crypto minor, 227
- data breaches, 200
- denial-of-service, 11, 181, 183, 186, 190
- downgrade, 126
- eavesdropping, 90
- elevation of privilege, 203
- firmware modification, 178
- flooding, 183
- invisible manipulation, 14
- jamming, 182
- log manipulation, 230
- malicious software, 143
- man-in-the-middle, 44
- mix-and-match, 154
- phases, 224
- physical access, 13, 200
- physical transfer, 105
- privilege escalation, 98
- public-key replacement, 145
- resource exhaustion, 186
- supply chain, 143
- SYN flooding, 194, 195
- theft of signing key, 148
- unknown methodologies, 160
- update misuse, 179

attribute-based access control (ABAC), 201

Aumasson, Jean-Philippe, 48

authenticated boot, 144

authenticated encryption (AE), 37–38, 123, 155
- encrypt-and-MAC, 37
- encrypt-then-MAC, 38
- MAC-then-encrypt, 38

authenticated encryption with associated data (AEAD)
- AES-GCM, 38, 71
- ChaCha20-Poly1305, 40, 71, 78, 126, 136
  - RFC 8439, 40

authentication, 103, 106
- challenge-response, 52, 104
- chip, 105
- protocol, 104

authenticator, 104
- implicit, 106

B

banana principle, 160

banking, 224

Bernstein, Daniel J., 35, 40, 47, 82

Biden, Joe, xxiii

binary large object (BLOB), 91

biometric data, 86

blacklisting, 212

BLAKE2s, 59

block cipher modes of operation
- Cipher Block Chaining (CBC), 33–34, 37, 95
- Counter (CTR), 34, 56
- Electronic Codebook (ECB), 32–33
- Galois Counter mode (GCM), 38–39
- Offset Codebook (OCB), 40
- XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing (XTS), 95

block ciphers. *See also* Advanced Encryption Standard
- Data Encryption Algorithm, 29
- Data Encryption Standard, 29
- 3DES, 29, 127

Bluetooth, 70, 103, 112

bootloader, 142, 164, 167
- multistage, 168

boot process, 57, 142
- authenticated, 144
- chain, 143
- encrypted, 144
- high-assurance, 144
- measured, 144
- secure, 145. *See also* secure boot
- trusted, 144
- unlock feature, 149
- verified, 144

BSI (German Federal Office for Information Security), 58, 67

Building Security In Maturity Model (BSIMM), 5
business model, xxi, 199, 224
  marketplace, 200
  platform, 200
BusyBox, 217, 235

C

CA (certificate authority), 107, 116, 129
CAESAR competition, 40
CAN bus, 135, 182
Canonical, 166
  Ubuntu, 213
  Ubuntu Core, 166
card identification (CID), 112
case studies
  AppArmor, 214–221
  crypto performance, 75–83
  encrypted file container, 93–98
  identity generation, 111–117
  Linux access control, 207–210
  logging, 231–236
  MQTT security, 129–135
  randomness quick check, 63–67
  random number generation, 58–62
  robustness under stress, 192–197
  RSA key generation, 117–118
  secure boot, 149–154
  secure update, 170–179
CBC (Cipher Block Chaining), 33–34, 37, 95
central processing unit (CPU), 73, 142, 189
`cert_create`, 152
Certicom, 45
certificate, 106
  attributes, 116
  authority, 107, 116, 129
  chain, 107
  common name, 114–115, 130
  organization, 115
  self-signed, 116
  store, 127
  subject, 115
  validity period, 116
  verification, 133
  X.509, 107, 110, 124
    RFC 5280, 107
certificate authority (CA), 107, 116, 129
certificate revocation list (CRL), 107
certificate signing request (CSR), 111, 113–115
chain of trust (CoT), 152
Chaos Computer Club (CCC), 110
Chinese remainder theorem (CRT), 75
  Euler's phi function, 42
  factorization problem, 42
  modulus, 41
  private exponent, 42
  public exponent, 41
  square-and-multiply, 42, 74
Chromium, 19
CIP-007-6, 224
cipher-based message authentication code (CMAC), 37
Cipher Block Chaining (CBC), 33–34, 37, 95
ciphertext, 29, 43
Cisco, 110
Cloudflare, 54
code review, 20
common vulnerabilities and exposures (CVEs), 19, 24
communication
  low-level, 226
  network, 226
communication preprocessor, 187
Compression Ratio Info-Leak Made Easy (CRIME), 127
continuous integration (CI), 20, 147
controller area network (CAN) bus, 135, 182
controller cycle, 184
coprocessor, 164
copy-in-and-out (CPIO), 174
core pinning, 188, 192
CPU (central processing unit), 73, 142, 189
CRIME (Compression Ratio Info-Leak Made Easy), 127
Critical Infrastructure Protection (CIP), 224
crypto agility, 72, 168
cryptographic acceleration and assurance module (CAAM), 91

cryptographic material, 86
cryptography, 27
  asymmetric, 40
  ciphertext, 29, 43
  elliptic-curve, 45, 71
  implementations, 69
  plaintext, 29, 43
  post-quantum, 48
  public-key, 40
  search space, 28
  security level, 28
  symmetric, 29
  trapdoor function, 41
  white-box, 92
crypto implementations, 69
  accelerators, 79
  AES, 73
  balanced, 73
  benchmarking, 94
  bignum arithmetic, 74
  case study, 75–83
  data width, 73
  dynamic memory usage, 71
  energy consumption, 71
  latency, 70
  loop unrolling, 73
  maintenance, 72
  multiple-precision arithmetic, 74
  performance, 70, 128
  sanity checks, 80
  software vs. hardware, 78
  static code size, 71
  throughput, 70
  transparency, 72
CSR (certificate signing request), 111, 113–115
CTR (Counter), 34, 56
customer complaints, 224
CVEs (common vulnerabilities and exposures), 19, 24
cyber kill chain, 224
Cyber Resilience Act (CRA), xxiii
Cybersecurity Act (CSA), xxiii
cyclic redundancy check (CRC), 9, 136

D

DAC (discretionary access control), 203
data analytics, xxi, 121, 223
data-driven service, xxi
Data Encryption Algorithm (DEA), 29
data encryption key (DEK), 91
Data Encryption Standard (DES), 29
Datagram Transport Layer Security (DTLS), 128
DDR (double data rate), 142–146
debug port, 201
decommissioning, 203
defense in depth, 17, 201, 237
DEK (data encryption key), 91
denial of service (DoS), 11, 181, 183, 186, 190
deobfuscation, 92
DES (Data Encryption Standard), 29
Designing Secure Software (Kohnfelder), 25
deterministic random bit generator (DRBG), 56, 58. *See also* pseudorandom number generator
device identity, 101–119. *See also* identity
device life cycle, 199
device tree, 153, 164
device tree blob (DTB), 153
`devmem2`, 111
Dieharder suite, 63
Diffie, Whitfield, 43
Diffie-Hellman (DH), 43–44, 126
Diffie-Hellman Ephemeral (DHE), 45, 125–126, 136
digital forensics, 224, 230
digital signature, 40–41, 135, 172, 174, 178
digital video recorder (DVR), 148
discrete logarithm problem (DLP), 44
discretionary access control (DAC), 203
double data rate (DDR), 142–146
DRBG (deterministic random bit generator), 56, 58. *See also* pseudorandom number generator
Dropbear, 210, 233, 235
  command line arguments, 210
  /etc/dropbear/default, 211, 234
DTB (device tree blob), 153
DVR (digital video recorder), 148
dynamic application security testing (DAST), 20

E

ECB (Electronic Codebook) mode, 32–33
ECC. *See* elliptic-curve cryptography
Eclipse Foundation, 129, 131
Eclipse hawkBit, 169, 175
Eclipse Mosquitto, 129, 210
Eclipse Paho, 131
Elastic Stack, 231
electronics manufacturing services (EMS) provider, 108
elliptic-curve cryptography (ECC), 45, 71
- discrete logarithm problem, 46
- security, 46

Elliptic-Curve Diffie-Hellman (ECDH), 47
Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE), 47, 125–126, 136
Elliptic-Curve Digital Signature Algorithm (ECDSA), 47, 71, 75, 82, 145, 151
Elliptic-Curve Integrated Encryption Scheme (ECIES), 48
elliptic curves
- Brainpool P521t1, 82
- Curve25519, 45, 47, 82
- Curve41417, 47
- double-and-add, 46
- Ed448-Goldilocks, 46, 47
- Edwards curves, 46
- Montgomery curves, 45
- NIST-P-192, 47
- NIST-P-224, 47, 82
- NIST-P-256, 45, 47, 82, 126
- NIST-P-384, 47
- NIST-P-521, 47, 82
- point addition, 46
- point doubling, 46
- scalar multiplication, 46
- Weierstrass curves, 45

embedded MultiMediaCard (eMMC), 142
embedded system
- application domains, xxi
- battery powered, 228
- constraints, xxii, 135, 223, 228
- security, xxii

EMS provider, 108
encrypted boot, 144
encrypted salt-sector initialization vector (ESSIV), 96
ENISA (European Union Agency for Cybersecurity), 5
Enrollment over Secure Transport (EST), 110
entropy source, 54
- health status, 55
- online test, 55
- postprocessing, 58
- startup test, 55
- total failure test, 55

error-correcting codes, 136
error-detecting codes, 136
errors, 227, 236
essential functions
- actuators, 184
- controllers, 184
- sensors, 183

ESSIV (encrypted salt-sector initialization vector), 96
Ethernet, 70, 103, 112, 182, 192
- PHY, 187
- ring topology, 136

ETSI EN 303 645, xxiii, 202
European Union Agency for Cybersecurity (ENISA), 5
Executive Order 14028, xxiii

F

fault injection, 240
Feistel network, 29
field-programmable gate array (FPGA), 70, 73, 93, 142, 187, 188
- bitstream, 164

file-based encryption (FBE), 88
file container, 88, 94
- case study, 93–98

Filesystem in Userspace (FUSE) framework, 88
filesystems
- activities, 225
- compressed, 98
- CramFS, 98, 155
- eCryptfs, 88
- EncFS, 88, 155
- encrypted, 87, 229

filesystems *(continued)*
- ext2, 97
- ext3, 88, 96, 155
- ext4, 88, 98, 155, 170
- extended file attributes, 207
- F2FS, 88
- gocryptfs, 88, 155
- integrity, 141, 155
- native, 88
- permissions, 204
- read-only, 98, 155
- SquashFS, 98, 155
- stacked, 88, 155
- UBIFS, 88

`fiptool`, 151
firewall, 191, 224
firmware, 164
- image, 170, 177
- image package, 151
- signing, 147, 150
- update, 159, 169, 203

first-stage bootloader (FSBL), 142, 146, 150
Flattened Image Tree (FIT), 152
FPGA. *See* field-programmable gate array
Free Software Foundation (FSF), 148
full-disk encryption (FDE), 88
fully qualified domain name (FQDN), 124
functional safety, 15, 136, 159
FUSE framework, 88

G

Galois field, 45
Galois Counter mode (GCM), 38–39
General Data Protection Regulation (GDPR), 10, 86, 224, 231
general-purpose input/output (GPIO), 226
geo-fencing, 106
German Federal Office for Information Security (BSI), 67
- AIS-32, 58

Ghidra, 87
GID (group identifier), 206
globally unique identifier (GUID)
- RFC 4122, 103

GNU General Public License (GPL)
- version 2, 148
- version 3, 148

GNU Grand Unified Bootloader (GRUB), 149, 168
Google, 144
- Chrome OS, 88, 144, 156

GPIO (general-purpose input/output), 226
graphics processing unit (GPU), 93, 142
Graylog, 231
group identifier (GID), 206
GUID (globally unique identifier), 103
- RFC 4122, 103

H

Hacking the Xbox (Huang), xxii
Hamming codes, 136
Hardware Hacking Handbook, The (Woudenberg and O'Flynn), 83, 240
hash-based message authentication code (HMAC), 36–37, 56, 93, 155
- HMAC-SHA-256, 37
- RFC 2104, 36

hash functions, 56
- birthday paradox, 35
- collision resistance, 35
- digest, 35
- hash value, 35
- preimage resistance, 35
- rho method, 35
- second preimage resistance, 35

hash tree, 156
hawkBit, 129, 131, 169, 175
health status, 227
Hellman, Martin, 43
high-assurance boot, 144
HMAC (hash-based message authentication code), 36–37, 56, 93, 155
HMAC-based extract-and-expand key derivation function (HKDF), 126
`hping3`, 194, 195
Huang, Andrew, xxii
human factor, 6, 240
HyperText Transfer Protocol (HTTP), 123
- over TLS, 128

- HyperText Transfer Protocol Secure (HTTPS), 128
- hypervisor, 189

I

- I^{2}C (Inter-Integrated Circuit) bus, 200, 206
- ICS (industrial control system), xxiii
- identification, 102
- identifiers, 102–103, 111, 113
- identity (ID)
  - backup, 108, 109
  - case study, 111–117
  - destruction, 111
  - exchange, 110
  - generation, 108, 111
  - life cycle, 108
  - management, 107
  - plausibility checks, 110
  - provisioning, 109, 111
  - uniqueness, 102
- identity-based access control (IBAC), 201
- IEC (International Electrotechnical Commission), 4
- IEC 62439, 137
- IEC 62443, xxiii, 4, 143, 160
  - certification, 5, 16
  - Part 4-1, xxiv, 4
  - Part 4-2, xxiv, 16, 183, 224
  - security level, 143
- IEEE 802.1AE, 137
- Image Tree Source (ITS) file, 152
- implicit authenticator, 106
- incident response, 231
- indicator of compromise (IoC), 231
- industrial, scientific, and medical (ISM) radio band, 135
- industrial control system (ICS), xxiii
- industrial internet of things (IIoT), xxiii, 122
- Infineon OPTIGA Trust X, 90
- initialization vector (IV), 34
- “In Practice” boxes
  - discarding features, 18
  - penetration-testing goals, 22
  - planning for security, 19
  - security engineering experts, 5–6
  - threat-modeling workshops, 10–11
  - vulnerability reporting, 24
- input validation, 191
- insecure channel, 43
- insecurity by design, xxiii
- instruction set architecture (ISA), 70
- Intel, 91, 144
- intellectual property, 85, 122, 143
- Inter-Integrated Circuit (I^{2}C) bus, 200, 226
- International Electrotechnical Commission. *See* IEC
- internet of things (IoT), xxii, 72, 90, 122, 129, 160, 199
- Internet Protocol (IP), 123
- Internet Protocol security (IPsec), 137
- intrusion detection system (IDS), 224
- IP address, 226, 231, 235
- ISM (industrial scientific, and medical) radio band, 135
- ISO/IEC 18033-3, 30
- ITS (Image Tree Source) file, 152

J

- Joint Test Action Group (JTAG), 156, 200

K

- Keccak, 36
- Kerckhoffs, Auguste, 28
- Kerckhoffs’s principle, 28
- key
  - cryptographic, 29, 85, 164
  - decryption, 161
  - ephemeral, 45
  - generation, 52, 57, 172
  - private, 40, 127, 129, 147, 229
  - public, 40, 135, 229
  - secret, 29
  - test-signing, 147
- keyed hash function, 36. *See also* hash-based message authentication code
- key exchange
  - anonymous Diffie-Hellman, 44, 127
  - authenticated Diffie-Hellman, 44
  - Diffie-Hellman, 43–44, 126
  - Diffie-Hellman Ephemeral, 45, 125–126, 136

- key exchange *(continued)*
  - Elliptic-Curve Diffie-Hellman, 47
  - Elliptic-Curve Diffie-Hellman Ephemeral, 47, 125–126, 136
  - key agreement, 43
  - key transport, 43
  - pre-shared key, 125
  - RSA, 127, 134
  - X25519, 126
- Kohnfelder, Loren, 25
- Kuster, Armin, 215

L

- least privilege, 17, 201
- Let's Encrypt, 110
- LibreTLS, 71
- lifetime data, 85
- Lightweight Directory Access Protocol (LDAP), 203
- linear feedback shift register (LFSR), 56
- Linux, 189
  - `add_device_randomness`, 60
  - `add_disk_randomness`, 60
  - `addgroup`, 206
  - `add_hwgenerator_randomness`, 60
  - `add_input_randomness`, 60
  - `adduser`, 206
  - AKARI, 214
  - AppArmor, 213–215, 232
  - `apt-get`, 166
  - `audisp`, 236
  - `audisp-remote`, 236
  - `auditbeat`, 236
  - `auditctl`, 233
  - `auditd`, 232, 234, 236
  - audit framework, 232
  - `ausearch`, 234
  - automotive-grade, 214
  - block device, 88
  - *bootid*, 60
  - `bzip2`, 64
  - `chgrp`, 206
  - `chmod`, 206
  - `chown`, 206
  - crypto API, 88
  - `cryptodev`, 79
  - `cryptsetup`, 88, 94
  - `cyclictest`, 193–195
  - `dd`, 61, 95
  - */dev/hwrng*, 58, 209
  - */dev/mmcblk0*, 209
  - */dev/random*, 61
  - */dev/urandom*, 61, 95, 209
  - `df`, 97
  - directories, 205, 208
  - `dm-crypt`, 88, 155
  - `dmesg`, 219
  - `dm-integrity`, 155
  - `dm-verity`, 156
  - entropy pool, 59
  - */etc/passwd*, 209, 220, 233
  - */etc/shadow*, 209, 234
  - `fdisk`, 97
  - file container, 88, 94
  - filesystem permissions, 204
  - `fscrypt`, 88
  - `getfacl`, 207
  - `getrandom`, 61
  - `get_random_bytes`, 61
  - `grep`, 231
  - `GRND_INSECURE`, 61
  - `groupadd`, 205, 206
  - `groupdel`, 205
  - group identifier, 206
  - `groupmod`, 205
  - `gzip`, 64
  - `httpd`, 210, 216
  - `hw_random`, 58
  - `ibm-tss`, 90
  - `journalctl`, 178, 179, 231
  - `journald`, 231, 236
  - kernel, 143, 164, 212, 232
  - kernel module verification, 154
  - */lib/firmware/*, 196
  - Linux Security Module, 212
  - Linux Unified Key Setup, 88, 94, 97
  - low-latency kernel, 193–194
  - `ls`, 204, 217
  - `lsblk`, 177, 178
  - LUKS1, 97
  - LUKS2, 97
  - `mke2fs`, 96
  - `mosquitto`, 210
  - `mount`, 96
  - `opkg`, 166

partition, 88
PREEMPT, 193
preemption, 190
PREEMPT_RT, 190, 193
/proc/cpuinfo, 112
proc filesystem, 60
/proc/sys/kernel/random/uuid, 60
ps, 210
remoteproc, 196
remote processor messaging, 197
RNG, 59, 64, 103
rngtest, 59
rng-tools, 59
root user, 204, 207
rsyslog, 236
scheduling, 190, 193–194
SELinux, 212, 232
setfacl, 207
setgid(), 210
setuid(), 210
SMACK, 214
SMP, 193
sysfs, 196
syslog, 236
syslogd, 217, 235
syslog-ng, 236
systemctl, 216
systemd, 175, 231
systemd-journal-remote, 236
time, 81
TOMOYO, 214
touch, 234
tpm2-tools, 90
uImage, 170
uname, 193, 195
useradd, 205–207
userdel, 205
user identifier, 205
usermod, 205
/var/log/messages, 235
veritysetup, 156
xz, 64
zImage, 153
logging, 223
architecture, 228
capacity, 230
case study, 231–236
central, 230, 236
limits, 230
off-loading, 228
on-device, 236
login attempt, 235
low-level communication, 226
LSM (Linux Security Module), 212
LUKS (Linux Unified Key Setup), 88, 94, 97
header, 97

M

mandatory access control (MAC), 211, 232
Mangard, Stefan, 83, 240
man-in-the-middle (MITM), 44
Mbed TLS, 52, 71, 128, 152
measured boot, 144
media access control (MAC)
MAC address, 103, 112, 231
MACsec, 137
memory
double data rate (DDR), 142
internal flash, 156
nonvolatile, 142
read-only memory (ROM), 142, 146, 150
volatile, 142
Mender, 169
message authentication code (MAC)
authentication tag, 36
cipher-based message authentication code (CMAC), 37
hash-based message authentication code (HMAC), 36–37, 56, 93, 155
message integrity code (MIC), 36
Poly1305, 40
Microchip ATECC608B, 90
microcontroller, 70, 72, 98, 187, 228
read-out protection, 99
write protection, 156
Microsoft, 13, 19
BitLocker, 90
SDL, 4
Windows, 90, 144
Mirai botnet, xxii
mkimage, 154

Modbus, 123
monitoring, 223, 225
- architecture, 228
- experts, 231
- on-device, 228
- remote, 228, 236
- scalability, 231
- scheme, 228

MQTT
- broker, 129, 210
- case study, 129–135
- client, 131
- protocol, 129, 132
- publish, 131
- subscribe, 131

multicore architecture, 188
multifactor authentication (MFA), 105

N

National Institute of Standards and Technology (NIST), xxiii, 5
- FIPS 140-2, 59
- FIPS 180-4, 36
- FIPS 186-5, 47
- FIPS 197, 30
- FIPS 202, 36
- post-quantum cryptography, 48
- SP 800-160, 5
- SP 800-22, 63
- SP 800-38A, 32
- SP 800-38C, 38, 40
- SP 800-56A, 45, 47
- SP 800-56B, 43
- SP 800-57, 42, 46
- SP 800-90A, 56
- SP 800-90B, 54

Netscape, 123
network
- communication, 226
- load, 182
- packet filtering, 187
- ring topology, 136
- stress, 182
- traffic monitoring, 224
- traffic preprocessing, 187

Network Time Protocol (NTP), 128, 229
NIST. *See* National Institute of Standards and Technology
`nmap`, 130, 186, 194, 196
nonce (number used once), 34
nondeterministic random bit generator (NRBG), 53–55
Norris, Chuck, 209
North American Electric Reliability Corporation (NERC), 224
NXP
- cryptographic acceleration and assurance module, 91
- EdgeLock SE050, 90
- i.MX series, 91, 144

O

OAEP (Optimal Asymmetric Encryption Padding), 43
obfuscation, 92, 201
Offset Codebook (OCB), 40
O'Flynn, Colin, 83, 240
one-time programmable (OTP) memory, 91, 146, 151
Online Certificate Status Protocol (OCSP), 107
OpenSSL, 71, 76, 128, 129, 134, 155
- `openssl ciphers`, 134
- `openssl genrsa`, 116, 152, 172
- `openssl passwd`, 207
- `openssl req`, 115–116, 152
- `openssl rsa`, 172
- `openssl speed`, 76
- `openssl x509`, 116

Open Systems Interconnection (OSI) model, 122, 137
Open Web Application Security Project (OWASP), 4
- OWASP Top 10, 20

operating system (OS), 19, 20, 57, 59, 81, 154, 164, 189, 202, 211
OP-TEE, 151
Optimal Asymmetric Encryption Padding (OAEP), 43
OSI (Open Systems Interconnection) model, 122, 137
OSTree, 169
Oswald, Elisabeth, 83, 240
OT:ICEFALL, xxiii

OTP (one-time programmable) memory, 91, 146, 151
OTP master key (OTPMK), 91
over-the-air (OTA), 162, 175
OWASP. *See* Open Web Application Security Project

P

Paar, Christof, 48
partition layout, 166, 170
passphrase, 89
password
  default, 202
  device-individual, 202
  file, 130
  hash, 93
  rainbow tables, 93
  salt, 93
  shadowing, 209
  storage, 93
Password-Based Key Derivation Function 2 (PBKDF2), 93
  RFC 2898, 93
Password Hashing Competition, 93
patch management, 163
PCB (printed circuit board), 14, 18, 90–91, 105, 142, 164, 201
Pelz, Jan, 48
penetration test, 21–22
perceptual beta, 160
perfect forward secrecy (PFS), 45
personal data, 122
personally identifiable information (PII), 231
physical security, 224
physical unclonable function (PUF) 102
PKI (public-key infrastructure), 107, 128
plaintext, 29, 43
PLC (programmable logic controller), xxvi, 184
Popp, Thomas, 83, 240
Power Analysis Attacks: Revealing the Secrets of Smart Cards (Mangard, Oswald, and Popp), 83, 240
Precision Time Protocol (PTP), 128
predictive maintenance, 7, 121, 223
preemption
  `PREEMPT`, 193
  `PREEMPT_RT`, 190, 193
pre-shared key (PSK), 125
privacy, 10, 122, 203, 224
Privacy-Enhanced Mail (PEM), 87
PRNG. *See* pseudorandom number generator
Probabilistic Signature Scheme (PSS), 43, 126
  RFC 3447, 43
processor affinity, 188
product housing, 200
  contact spring, 201
  contact switch, 201
  label, 202
  mesh structure, 201
production, 22, 108, 117, 148, 202
product security officer (PSO), 5
programming languages
  C, 19, 20
  C++, 19
  Python, 58, 62, 129, 218
  Rust, 19, 128
protection goals
  anonymity, 10
  authenticity, 9, 37, 40, 122, 135, 143, 154, 161, 191
  availability, 9, 122, 136, 181, 197
  confidentiality, 9, 29, 37, 40, 85, 122, 144, 161, 201, 229
  integrity, 9, 36–37, 40, 122, 135, 143, 154, 229
  nonrepudiation, 9
  privacy, 10, 122, 203, 224
  pseudonymity, 10
protocol design, 135, 190
pseudorandom number generator (PRNG)
  backtracking resistance, 56
  CTR_DRBG, 56
  Dual_EC_DRBG, 56
  Hash_DRBG, 56
  HMAC_DRBG, 56
  linear feedback shift register, 56
  Mersenne Twister, 56, 62
  non-cryptographic, 56
  prediction resistance, 56

pseudorandom number generator *(continued)*
- reseeding, 57
- seeding, 56

PSK (pre-shared key), 125
PSS. *See* Probabilistic Signature Scheme
public-key infrastructure (PKI), 107, 128
Python, 58, 62, 129, 218
- `cryptography`, 113, 118
- `os`, 62
- `os.urandom()`, 62
- `random`, 62
- `secrets`, 62
- `secrets.randbelow()`, 66
- `secrets.token_bytes()`, 62
- SSLyze, 132
- subprocess, 113

R

Radare2, 87
randomness
- bias, 53, 63–65
- case study, 63–67
- entropy, 52
- entropy source, 54
- independence, 53
- patterns, 53, 63, 67
- pseudo, 51
- source, 128
- true, 51, 53–56
- uniform distribution, 53, 63–64, 66

random number generator (RNG), 51, 128
- case study, 58–62
- hybrid, 57
- pseudo, 56. *See also* pseudorandom number generator
- true, 53, 55

ransomware, 11
RAUC, 169
real time, 9, 181
- firm, 185
- hard, 185
- soft, 185

real-time core, 188, 192, 196
real-time operating system (RTOS), 98, 156, 164, 189
reconnaissance, 236
redundancy, 136
remote access, 121
remote processor messaging (RPMsg), 197
removable media, 225
resource allocation
- dynamic, 186
- fixed, 186

reverse engineering, 14, 87, 91, 143, 156, 200
RFC 2104, 36
RFC 2898, 93
RFC 3447, 43
RFC 4122, 103
RFC 4493, 37
RFC 5246, 126
RFC 5280, 107
RFC 6960, 107
RFC 7914, 93
RFC 8439, 40
RFC 8446, 124
Rijndael, 30
ring oscillator (RO), 54–55
- jitter, 54

ring topology, 136
Ripple20, xxii, 160
Rivest-Shamir-Adleman (RSA), 41–48, 71, 81, 113, 126, 145, 152, 172
- case study, key generation, 117–118

RNG. *See* random number generator
RO. *See* ring oscillator
robustness
- case study, 192–197
- digital, 181
- physical, 181

Rogaway, Phil, 40
role-based access control (RBAC), 201
ROM (read-only memory), 142, 146, 150
root certificate, 107
root filesystem, 164
root hash, 156
RSA. *See* Rivest-Shamir-Adleman
RSAES-OAEP, 43
RSA-OAEP, 43
RSASSA-PSS (RSA Signature Scheme with Appendix), 126

RTOS (real-time operating system), 98, 156, 164, 189
runtime data, 165
Rustls, 128

S

safety, 15, 136, 159
SAMM (Software Assurance Maturity Model), 4
Samsung Tizen, 214
scrypt, 93
SDL (secure development life cycle), 3, 22
second-stage bootloader (SSBL), 142, 146, 150
secure boot, 141, 144
  case study, 149–154
  chain, 145
  hardware vulnerabilities, 154
  implementation, 146
  open source licenses, 148
  testing, 148, 154
secure channel, 43
secure coding rules, 19, 190
secure communication, 121, 229
secure development process. *See also* security: testing; vulnerability management
  education, 4
  governance, 4
  guidelines, 4
  life cycle, 3, 22
  management, 4
  principles, 17
  responsibility, 5
  secure implementation, 18
  shift left, 18
  threat assessment, 4
  threat modeling, 4
  training, 4, 6
  transparency, 5, 18, 20, 224
  validation, 4, 18
  verification, 4, 18
Secure Hash Algorithm (SHA)
  SHA-1, 35, 59, 93, 123
  SHA-2, 36
  SHA-3, 36
  SHA-224, 79
  SHA-256, 36, 78–81, 96, 123, 126, 134–135, 151, 153, 173
  SHA-384, 36, 127, 153
  SHA-512, 36, 93, 153
  SHA3-224, 36
  SHA3-256, 36
  SHA3-384, 36
  SHA3-512, 36
secure memory, 89
secure secret provisioning (SSP), 151
Secure Shell (SSH), 57, 137, 210, 226, 235
Secure Sockets Layer (SSL), 123
secure update, 159, 169
  A/B system, 167–168
  atomicity, 165
  case study, 170–179
  complexity, 213
  containers, 165
  downgrade, 169
  encryption, 161, 169
  file, 170
  image, 165
  labels, 212
  local, 162, 175
  modes, 216
  over-the-air, 162, 175
  package manager, 166
  pull strategy, 163
  push strategy, 163
  recovery partition, 166, 168
  rollback protection, 161
  type enforcement, 212
  version monitoring, 162
security. *See also* secure update
  architecture, 16
  awareness, 6
  by design, 5
  by obscurity, 28, 92, 98
  requirements, 16
  testing, 4, 18
    black box, 21
    chaos engineering, 192
    dynamic application security testing, 20
    fuzzing, 182, 192
    gray box, 21
    penetration testing, 21–22

security *(continued)*
testing *(continued)*
scanning, 130, 132, 182, 186
static application security testing, 20
white box, 21
security information and event management (SIEM), 231
SELinux (Security-Enhanced Linux), 212, 232
sender validation, 191
separation of duties, 197
serial number, 103, 111
Serious Cryptography (Aumasson), 48
SHA. *See* Secure Hash Algorithm
shared secret, 43
shift left, 18
Shostack, Adam, 25
side-channel analysis, 240
Simple Certificate Enrollment Protocol (SCEP), 110
Simplified Mandatory Access Control Kernel (SMACK), 214
SoC (system-on-chip), 70, 142, 146, 187
software applications, 164, 190, 200, 202, 210, 226
Software Assurance Maturity Model (SAMM), 4
software bill of materials (SBOM), 20
software libraries, 20
software segmentation, 240
software update. *See* secure update
Splunk, 231
SSBL (second-stage bootloader), 142, 146, 150
SSH (Secure Shell), 57, 137, 210, 226, 235
SSL (Secure Sockets Layer), 123
SSLyze, 131–134
ST. *See* STMicroelectronics
Stallman, Richard, 148
static application security testing (SAST), 20
STM32 Cube IDE, 196
STM32 Cube Programmer, 151, 170
STM32MP157F, 58, 75, 94, 149, 196
CRYP1, 76
HASH1, 76, 79
MAC unit, 192
STM32MP157F-DK2, xxvi, 60, 129, 170, 177, 214, 231
STM32MP Crypto Lib, 152
STM32MP Key Generator, 151
STM32MP Signing Tool, 151
STMicroelectronics (ST), xxvi, 58, 90, 149–150, 170
RM0436, 58, 81, 192
stream ciphers
ChaCha20, 34, 40, 59, 78
RC4, 127
Salsa, 35
STRIDE checklist, 13
Stuxnet, xxiii
surveillance, 223
SUSE Linux, 213
swupd, 169
SWUpdate, 159, 169, 170
`meta-swupdate`, 171, 173
mongoose mode, 175
post-update commands, 176
pre-update commands, 176
suricatta mode, 175
sw-description, 172
sw-description.sig, 174
`swupdate`, 174, 178
swupdate.cfg, 175
`swupdate-www`, 174
web interface, 178
symmetric multiprocessing (SMP), 188
system crashes, 227, 230
system identity, 103
system integrity, 9, 141, 221, 229
system-on-chip (SoC), 70, 142, 146, 187
system utilization, 227

T

Tab-Separated Values (TSV), 170
tamper detection, 89
TCP (Transmission Control Protocol), 123, 192
TCP/IP stack, 160, 187
TEE (trusted execution environment), 142, 151
telematics infrastructure, 110
third-party applications, 227

third-party dependencies, 20
threat modeling, 179. *See also* attackers; protection goals; threats
  assets, 7, 10
  device overview diagram, 8
  multidimensional, 8
  risks, 11, 14–15, 227
  risk treatment, 16
  software, 16
  STRIDE, 13
  system understanding, 7
  workshops, 10, 14
Threat Modeling: Designing for Security (Shostack), 25
threats
  attack vectors, 11
  potential impact, 15
  probability of occurrence, 15
  risk score, 15
  threat actors, 11. *See also* attackers
  threat scenarios, 11–15
  vulnerabilities, 11
time
  base, 128, 229
  server, 229
  synchronization, 229
Time-Sensitive Networking (TSN), 137
timestamps, 229
TiVo, 148
tivoization, 148
TPM. *See* Trusted Platform Module
Transmission Control Protocol (TCP), 123, 192
Transport Layer Security (TLS), 123, 161
  `Application Data`, 132
  cipher suite, 126–127, 132–133
  `ClientHello`, 125, 132
  `Finished`, 125
  handshake protocol, 124, 132
  history, 123
  mutual authentication, 125, 161
  `NULL` cipher, 127
  record protocol, 124
  requirements, 127
  RFC 5246, 126
  RFC 8446, 124
  `ServerHello`, 125, 132
  TLS 1.2, 126
  TLS 1.3, 124
  `Version`, 132
  zero round-trip time, 126
trapdoor function, 41
Triple DES (3DES), 29, 127
TrueCrypt, 88
true random number generator (TRNG), 53–55
trust, 55, 106, 129, 143
trusted boot, 144
Trusted Computing Group (TCG), 144
trusted execution environment (TEE), 142, 151
Trusted Platform Module (TPM), 90–91, 144
  firmware, 91
  integrated, 91
  TPM 2.0 specification, 90
trusted third party (TTP), 106, 110
TSV (Tab-Separated Values), 170

U

UART (Universal Asynchronous Receiver-Transmitter), 200
U-Boot, 142, 149–150, 152
  extlinux.conf, 171, 177, 215
  `stm32key`, 151
UDP (User Datagram Protocol), 123, 128, 192
UID (unique ID), 111, 205
Understanding Cryptography (Paar and Pelzl), 48
UN Regulation 155, 224
UN Regulation 156, 160
Urgent/11, 160
user
  admin, 202
  context, 202
  credentials, 200
  interaction, 225
  owner, 203
  permissions, 199
  restriction, 200
  roles, 199, 201
  root, 204
  separation, 199
  sessions, 225

US FD&C Act, 160
UUID (universally unique identifier), 60, 103, 171
    RFC 4122, 103

V

van Woudenberg, Jasper, 83, 240
VeraCrypt, 88
verified boot, 144
virtual local area network (VLAN), 192
virtual private network (VPN), 137
Voice over IP (VoIP), 128
vulnerability management, 200, 231
    monitoring, 23, 169
    reporting, 22

W

warnings, 227
web server, 110, 128, 202, 210, 226, 236
white-box cryptography, 92
whitelisting, 211
Wi-Fi, 8, 70, 103, 112, 182
Wireshark, 132
wolfSSL, 71

X

xattr (extended file attributes), 207
XTS (XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing), 95

Y

yescrypt, 93
Yocto Project
    `bitbake`, 195
    `debug-tweaks`, 207
    deploy, 174
    `extrausers`, 207
    `meta-oe`, 232
    `meta-security`, 215
    `meta-st-x-linux-rt`, 194
    `meta-swupdate`, 171, 173
    `mosquitto` recipe, 129
    OpenSTLinux, xxvi, 215
    `st-image-core`, 174, 193, 207
    `useradd`, 207

Z

zero round-trip time (0-RTT), 126