Index

A

Access, 30, 41
- control, 29, 401–402
- threats, 41

Accessibility, 223
Access point (AP), IEEE 802.11, 233
Access policy, 412–413
Access requestor (AR), 161
- supplicants, 161

Accidental association, 224
Account or service hijacking, 178
Active attacks, security, 25–27
Add Round Key
- AES, 57
- algorithm, 56–59
- Data Encryption Algorithm (DEA), 52
- Data Encryption Standard (DES), 52–55
- decryption, defined, 47, 97
- Diffie–Hellman key exchange, 104–107
- Digital Signature Algorithm (DSA), 108
- elliptic curve cryptography (ECC), 109
- encryption, 47, 96
- mix columns, 59
- public-key cryptography, 96–100
- RSA public-key encryption, 101–103
- state array, 56
- structure, 56
- subkey generation, 52
- substitution bytes, 56
- symmetric block encryption, 52–59
- triple Data Encryption Standard (3DES), 54–55

Ad hoc networks, 224
Advanced Encryption Standard (AES), 52, 55–59
Advanced persistent threats (APTs), 341–342
AES. *See* Advanced Encryption Standard (AES)
Algorithms, 46, 52–59, 62–63, 100–109, 273–274, 316
- cryptographic, 273–274
- ESP, 316
- HMAC, 91–93
- S/MIME, 273–274

Anti-replay service, ESP, 316–317
Application-level gateway, 419
Application proxy, 419
Architecture, 24–25
- open systems interconnection (OSI), 24–25

Attack(s), 25–27. *See also* Cryptanalysis*;* Security attacks*;* Threats
- active, 27
- chosen plaintext, 49
- ciphertext only, 48
- denial-of-service (DoS), 30
- insider, 379
- intruder, 377
- kits, 340
- known plaintext, 49
- man-in-the-middle, 107–108
- messages, types of for, 49
- passive, 25
- password, 135–136
- security, 25–27
- source routing, 417
- sources, 340–341
- tiny fragment, 417–418

Attacking IRC chat networks, 357
Attack surfaces, 36–37
Attack trees, 37–39
Audit records
- detection-specific, 383
- field
  - action, 383
  - exception-condition, 383
  - object, 383
  - resource-usage, 383
  - subject, 383
  - time-stamp, 383–384
- native, 383

Authentication, 29, 79–84, 164, 189, 192–193, 215. *See also* Message authentication*;* Message authentication codes (MAC)
- applications, 119–155
- client/server exchange, 137
- data origin, 29, 32
- dialogues, 125–132
- forwarding, 135
- IEEE 802.11i phase, 237–240
- IKE key determination, 327–328
- Internet Protocol (IP), 323
- interrealm, 135
- Kerberos, 124–137
- key exchange client and server, SSL, 200–201
- message, 78–112
- methods, 164
- peer entity, 29
- pretty good privacy (PGP), 279–280
- public-key infrastructure (PKI), 146–149
- remote user, 120–122
- server (AS), 125, 166
- service exchange, 136
- X.509 service, 139

Authority key identifier, 145

B

Backdoor (trapdoor), 359
Barcode readers, 224
Barrier security, 230
Base-rate fallacy, 388–389
Basic service set (BSS), IEEE 802.11, 233–234
Bastion host, 421
Bcrypt, 400. *See also* Hash functions
Behavior-blocking software, 363
Block ciphers, 50, 52, 63–65
- cipher block chaining (CBC) mode, 68–70
- cipher feedback (CFB) mode, 70–71

defined, 48
design of, 50
electronic codebook (ECB), 68
modes of operation, 68
plaintext processing, cryptography, 48
Bloom filter, 404–406
Bogus reconfiguration commands. *See* Network injection
Boot sector infector, 346
Bots, uses of, 356–357
attacking IRC chat networks, 357
DDoS attacks, 356
installing advertisement add-ons and BHOs, 357
keylogging, 356
manipulating online polls/games, 357
sniffing traffic, 356
spamming, 356
spreading new malware, 356
Bring-your-own-device (BYOD) policy, 228
Broad network access, 171–172
Browser helper objects (BHOs), 357
Business continuity and disaster recovery, 184

C

Canonical form, MIME and S/MIME, 264
Certificates, 140–144, 148, 200–201, 278
certification authority (CA), 140, 147, 276, 278
client types, 208
enhanced security services, 278–279
extensions, 141
forward, 143
issuer, 140, 141, 146
key information, 141
path constraints, 146
period of validity, 141
policy information, 145
policy mappings, 146
public-key, 138–139
reverse, 143
revocation list (CRL), 144, 278
revocation of, 144
serial number, 141
signature, 141
signature algorithm identifier, 141
S/MIME, 278
subject, 141
unique identifiers, 141
user's, obtaining, 142–144, 278
version, 140–141
X.509, 139–146
Certificates-only message, S/MIME, 278
Certificate usage field, 285
Certification authority (CA), 138, 147
key distribution, 138
public-key infrastructure (PKI), 146–149
X.509 certificates, 139–146
Change Cipher Spec Protocol, 191, 194–195, 201
Channels, 215–216, 223
Cipher block chaining (CBC) mode, 68–70
Cipher feedback (CFB) mode, 70–71
Cipher suites, TLS, 207
Ciphertext, 48, 97
Circuit-level gateway, 419–420
Circuit-level proxy, 419
Clandestine user, intruders, 377
Clear signing, S/MIME, 277
Client/server authentication exchange, 137
Client-side vulnerabilities, 352–353
drive-by-download, 352–353
Cloud auditor, 175
Cloud-based applications, 226
Cloud broker, 175
service aggregation, 176
service arbitrage, 176
service intermediation, 176
Cloud carrier, 175
Cloud computing
abuse and nefarious use of, 177
control functions and classes, 185
deployment models
community cloud, 173
hybrid cloud, 173–175
private cloud, 173
public cloud, 173
elements, 171–174
measured service, 172
on-demand self-service, 172
rapid elasticity, 172
reference architecture, 174–176
resource pooling, 172–173
service models, 173
Infrastructure as a service (IaaS), 173
Platform as a service (PaaS), 173
Software as a service (SaaS), 173
Cloud consumer, 175
Cloud provider, 175
Cloud security
risks and countermeasures
abuse/nefarious use of cloud computing, 177
account or service hijacking, 178
data loss or leakage, 178
insecure interfaces and APIs, 177
malicious insiders, 177
shared technology issues, 177–178
unknown risk profile, 178
as a service
business continuity and disaster recovery, 184
data loss prevention (DLP), 183–184
elements, 184
e-mail security, 184
encryption, 184
identity and access management (IAM), 183
intrusion management, 184
network security, 184–185
security as a service (SecaaS), 182
security assessments, 184
security information and event management (SIEM), 184
web security, 184
Codebook, 68
defined, 68
electronic (ECB), 68
Code, message authentication (MAC), 211–212

- Communications channel (CC), 38
- Community cloud, 173
- Complete mediation, 33
- Components, IDES, 394–395
- Compression
  - S/MIME, 272–273
  - SSL, 192
- Computer-generated passwords, 403
- Computer security, defined, 20
- Confidentiality, 20–22, 45–73, 241, 271, 316, 320. *See also* Encryption
  - data, 20, 28, 29
  - Encryption data, 249
  - Internet Protocol (IP), 322
  - pretty good privacy (PGP), 279–280
  - traffic flow (TFC), 316
- Connection Protocol, SSH, 209, 215–219
- Connection, TLS, 192
- Controls access, 413–414
- Cookie exchange, 327
- Countermeasures
  - distributed intelligence gathering approaches, 366–367
  - host-based behavior-blocking software, 363
  - host-based scanners, 362–364
    - first-generation scanner, 362
    - fourth-generation scanner, 363
    - second-generation scanner, 362–363
    - third-generation scanner, 363
  - malware countermeasure approaches
    - detection, 361
    - generality, 361
    - global and local coverage, 361
    - identification, 361
    - minimal denial-of-service costs, 361
    - removal, 361
    - resiliency, 361
    - timeliness, 361
    - transparency, 361
  - perimeter scanning approaches, 364–365
    - egress monitors, 365
    - ingress monitors, 364–365
  - rootkit countermeasures, 364
  - spyware detection and removal, 364
  - worm countermeasures
    - filter-based worm containment, 365
    - payload-classification-based, 365
    - rate halting, 366
    - rate limiting, 366
    - signature-based worm scan filtering, 365
    - TRW scan detection, 366
- Credential service provider (CSP), 121–122
- CRL issuer, PKI, 148
- Cross-certification, PKI, 148
- Cryptanalysis, 48–50
- Cryptographic computations, 202–203
- Cryptography, 48, 99–100. *See also* Public-key cryptography
  - algorithms, 105–106
  - classification of systems, 48
  - cryptosystems, applications for, 99–100
  - encryption structure, 97–99
  - public-key, 96–109
  - requirements for, 100

D

- Data
  - confidentiality, 28, 29
  - integrity, 30
  - origin authentication, 29
- Data Encryption Standard (DES), 52–55
  - algorithm, description of, 53
  - strength of, 53–54
  - triple (3DES), 54–55
- Data loss prevention (DLP), 178, 183–184
- Data protection, cloud computing
  - attributes, 181
  - encryption scheme, 181
  - multi-instance model, 180
  - multi-tenant model, 180
  - NIST guidelines on security and privacy, 178–180
  - primary key, 181
  - relation, 181
  - tuples, 181
- Decryption algorithm, 47, 97
- Demilitarized zone (DMZ) networks, 423–425
- Denial-of-service (DoS) attack, 30
  - constructing attack network, 370–371
    - hit list, 371
    - local subnet, 371
    - random, 371
    - topological, 371
  - countermeasures, 371–372
    - detection and filtering, 371
    - prevention and preemption, 371
    - source traceback and identification, 371
  - defined, 225
  - direct, 369
  - flooding-based, 370
  - internal resource, 368
  - reflector, 369
- De-perimeterization, 227
- Detection-specific audit records, 383
- Device security, 228–230
- Diffie–Hellman key exchange, 104–105, 200, 202, 224
  - algorithm, 105–106
  - anonymous, 200
  - ephemeral, 200
  - fixed, 199
  - introduction to, 104–105
  - man-in-the-middle attack, 107
  - protocols, 107–108
- Digital Signature Algorithm (DSA), 108, 109
- Digital signatures, 108–112
  - generation and verification, 110–111
  - RSA, algorithm, 111–112
- Digital Signature Standard (DSS), 108
- Discovery phase, IEEE 802.11i, 240–242
- Distributed firewall, 426–427
  - configuration, 427–428
- Distributed intrusion detection
  - central manager module, 390–391
  - host agent module, 390
  - LAN monitor agent module, 390
- Distribution system (DS), IEEE 802.11, 233

DNS-based Authentication of Named Entities (DANE), 266–267, 284–286
for SMTP, 286
TLSA record, 284–285
DNS Security Extensions (DNSSEC), 266, 280–284
domain name system, 280–282
protocol, 282–284
Domain-based Message Authentication, Reporting, and Conformance (DMARC), 267–268
functional flow, 298
on receiver side, 296–298
reports, 299
on sender side, 296
DomainKeys Identified Mail (DKIM), 289–295
E-mail threats, 290–291
functional flow, 292–295
strategy, 291–292
Double bastion inline, 424, 428
Double bastion T, 428
Double encryption, 135
Dynamic Host Configuration Protocol (DHCP), 164

E

EAP-GPSK (EAP Generalized Pre-Shared Key), 165
EAP-IKEv2, 165
EAP-TLS (EAP Transport Layer Security), 165
EAP-TTLS (EAP Tunneled TLS), 165
Eavesdropping. *See* Man-in-the middle attacks
Economy of mechanism, 33
Electronic codebook (ECB), 68
Electronic data interchange (EDI), 145
Electronic mail security, 253–299
DomainKeys Identified Mail (DKIM), 289–295
instant messenger facility, 348
pretty good privacy (PGP), 279–280
Secure/Multipurpose Internet Mail Extension (S/ MIME), 268–279
Electronic monitoring, 397
Electronic user authentication
means of, 122
NIST model for, 121–122
Elliptic curve cryptography (ECC), 109
Elliptic curve digital signature algorithm (ECDSA), 109
E-mail formats, 258–266
E-mail security, 184
E-mail threats, 266–268
Encapsulating security payload (ESP), 314–321
algorithms, 316
anti-replay service, 316–317
format, 314–316
padding, 316
transport mode, 317–320
tunnel mode, 320–321
Encapsulation, 35
Encryption, 45–73, 81–82, 99–100, 104, 109, 137, 184, 225. *See also* Block ciphers*;* Public-key cryptography*;* Stream ciphers
Advanced Encryption Standard (AES), 52, 55–59
algorithms, 46, 52–59, 62–63, 100–109
block ciphers, 50, 52, 63–65
ciphertext, 97
cryptanalysis, 48–50
cryptography, 48
Data Encryption Standard (DES), 52–55
decryption algorithms, 97
digital signatures, 108
double, 135
end-to-end, 123
Feistel cipher structure, 50–52
introduction to, 46
key distribution, 123–124, 137–139
message authentication and, 78–112
National Institute of Standards and Technology (NIST), 42, 52, 87, 108
plaintext, 48–50, 97
propagating cipher block chaining (PCBC), 135
public-key, 96–109
RSA algorithm, 101–103
stream cipher, 48, 63–65, 70
symmetric, 46–52
symmetric block algorithms, 52–59
system dependence, 134
triple Data Encryption Standard (3DES), 54–55
End entity, PKI, 147
End-to-end encryption, 123
EnvelopedData, S/MIME, 275–276
Exchange format, Intrusion detection, 393–395
Exchanges, 136–137. *See also* Key exchange
authentication service, 136
client/server authentication, 137
Kerberos, 134–136
ticket-granting service, 136–137
Extended service set (ESS), IEEE 802.11, 234
Extensible Authentication Protocol (EAP), 164
authentication methods, 164–165
EAP-GPSK (EAP Generalized Pre-Shared Key), 165
EAP-IKEv2, 165
EAP-TLS (EAP Transport Layer Security), 165
EAP-TTLS (EAP Tunneled TLS), 165
exchanges, 165–168
authentication server, 166
EAP authenticator, 166
EAP passthrough mode, 166
EAP peer, 166
RADIUS, 166
layered context, 164
messages
code, 166
data, 167
flow in pass-through mode, 167
identifier, 166
length, 166
Extensible Markup Language (XML), 394
External business requirements, 227

F

Fail-safe default, 33–34
Feistel cipher structure, 50–52
File infector, 346
File sharing, 348
Filter-based worm containment, 365

Firewall, 164, 410–428
basing, 420–423
bastion host, 421
host-based, 421–422
personal, 422–423
characteristics and access policy, 412–413
application protocol, 413
IP address and protocol values, 412
network activity, 413
user identity, 413
location and configurations, 423–428
distributed, 426–427
DMZ networks, 423–425
summary of, 427–428
virtual private networks, 425–426
need for, 411–412
types of, 414–420
application-level gateway, 419
circuit-level gateway, 419–420
packet filtering, 414–418
stateful inspection, 418–419
Forward certificate, 143
Fourth-generation scanner, 363
Fragmentation, SSL, 192

G

GPS capability on mobile devices, 228
Group master key (PMK), IEEE 802.11i, 246–247

H

Hackers, 377–378
Handheld PDAs, 224
Handshake Protocol, 165, 197–199
Hashed passwords, 397–399
Hash functions, 82–91, 399–400
HMAC, 91–93
one-way, 82–84
requirements, 84–85
secure, 84–85
Secure Hash Algorithm (SHA), 87
SHA-1 secure functions, 87–91
simple, 85–86
strong collision resistance, 84
weak collision resistance, 84
Heartbeat Protocol, 204–205
HMAC, 91–93
algorithm, 92–93
design objectives, 91–92
Honeypots, 391–393
Host audit record (HAR), 390–391
Host-based firewalls, 421–422
Host-based scanners, 362–363
Host keys, SSH, 209–214
Host-resident firewall, 427
HTTPS, 188, 207–208
Human attack surface, 36–37
Hybrid cloud, 173

I

Identifier (ID), 395, 396, 398
Identity and access management (IAM), 183
Identity theft (MAC spoofing), 224
IEEE 802.11i LAN, 236–250
authentication phase, 239, 242–243
characteristics of, 236–237
connection termination, 240
discovery phase, 239–241
key management phase, 241, 244–246
phases of operation, 237–240
protected data transfer phase, 239, 248–249
pseudorandom function (PRF), 249–250
Robust Security Network (RSN), 237
IEEE 802.11 LAN, 230–236
association-related services, 235
message distribution, 235
network components, 233–234
protocol architecture, 231–233
IEEE 802.1X port-based network access control, 163, 168–170
EAP-Key, 170
EAP-Logoff, 170
EAPOL-EAP, 170
EAPOL-Start, 170
packet body, 170
length, 170
packet type, 170
protocol version, 170
terminology related to IEEE 802.1X, 170
802.1X access control, 170
Independent basic service set (IBSS), IEEE 802.11, 233
Information
access threats, 41
security, 18
Infrastructure as a service (IaaS), 173
Initialization, 192
PKI, 148
Insecure interfaces and APIs, 177
International Telecommunication Union (ITU), 24
Internet Architecture Board (IAB), 303
Internet banking server (IBS), 38
Internet Engineering Task Force (IETF)
standards from, 42
Internet key exchange (IKE), 325–333
cookies, 327
header and payload formats, 329–333
IKEv5 message exchange, 328–329
key determination protocol, 326–329
Internet mail architecture, 254–258
e-mail components, 254–256
e-mail Protocols, 256–258
Internet Protocol (IP), 134, 303–309. *See also* Internet Protocol security (IPsec)
authentication plus confidentiality, 322–323
combining security associations (SA), 322–325
cryptographic suites, 333–335
dependence, 134
encapsulating security payload (ESP), 314–321
Internet key exchange (IKE), 325–333
security (IPsec), 309–314

security association database (SAD), 309–311
security policy database (SPD), 309, 311–312
traffic processing, 312–314
Internet Protocol security (IPsec), 303–314
documents, 306–307
packets, 312–314
policy, 309–312
routing, 306
transport mode, 308
tunnel mode, 308–309
Internet security, 253–299
defined, 19
electronic mail, 253–299
Internet protocol (IP), 164, 303–309
Transport Layer Security (TLS), 165, 190–207
transport-level, 187–219
Internet Security Association and Key Management Protocol (ISAKMP), 325
Internet service provider (ISP), 411
Internet standards
Internet Architecture Board (IAB), 42
Internet Engineering Task Force (IETF), 42
RFCs, 42
Intruder behavior patterns
criminals, 378
hackers, 377–378
insider attacks, 379
Intruders, 375–406
behavior patterns, 377–379
intrusion detection
audit records, 383–384
base-rate fallacy, 388–389
distributed, 389–393
exchange format, 393–396
rule-based, 386–388
statistical anomaly detection, 384–386
intrusion techniques, 379–381
password management
bloom filter, 404–406
hashed passwords, use of, 397–400
selection strategies, 403–404
user choices, 400–403
vulnerability of, 396–397
Intrusion Detection Exchange Protocol (IDXP), 394
Intrusion Detection Message Exchange Format (IDMEF), 393
Intrusion Detection System (IDES), 386
audit records, 383–384
base-rate fallacy, 388–389
distributed, 389–393
exchange format, 393–396
functional components, 394–395
rule-based, 386–388
statistical anomaly detection, 384–386
Intrusion management, 184
Intrusion techniques
access control, 379–381
one-way function, 379
IP address spoofing, 417. *See also* Packet filtering firewall
IPSec protocols, 425
Isolation, 35. *See also* Security design principles
ITU-T Recommendation X.800, 24, 25, 27, 29–32

K

Kerberos, 124–137
authentication
dialogues, 125–133
forwarding, 135
server (AS), 125
service exchange, 136
client/server authentication exchange, 137
differences between versions 4 and 5, 134–136
double encryption, 135
encryption system dependence, 134
environmental shortcomings, 134–135
Internet protocol dependence, 134
interrealm authentication, 135
introduction to, 124
message byte ordering, 134
nonce, 136
options, 136
password attacks, 135–136
principal, 134
propagating cipher block chaining (PCBC) encryption, 135
realms, 133–134, 136
session keys, 135
technical deficiencies of, 135
ticket-granting server (TGS), 126–127
ticket-granting service exchange, 136–137
ticket lifetime, 134–135
times, 136
version 4, 125–133
version 5, 134–137
Key distribution, 126, 140–142, 242, 247–248. *See also* Exchanges; Private keys; Public keys
center (KDC), 123
certificate authority (CA), 138
hierarchy, 246
IEEE 802.11i management phase, 241, 246–249
permanent key, 123
pretty good privacy (PGP), 279–280
private key, 270
public-key certificates, 138
public-key distribution of secret keys, 138–139
session key, 123
wireless network security, 244–248
Keyed hash function. *See* Message authentication codes (MAC)
Key exchange, 104–108, 199–200, 212, 325–333
certificate messages for, 200–201
client authentication and, 201
Diffie–Hellman, 104–108, 199
Internet, 325–333
Internet (IKE) key determination protocol, 326–329
protocols, 107
RSA, 199
server authentication and, 200–201
SSH Transport Layer Protocol, 210–211
Key generation, 203, 213–214, 278
AP, 239
S/MIME, 278
Keylogger, 358
Keylogging, 356

Key management. *See* Key distribution
Key pair recovery, PKI, 148
Key pair update, PKI, 148
Keystream, defined, 64

L

Layering, 35. *See also* Security design principles
Least astonishment, 36
Least common mechanism, 34
Least privilege, 34
Limitations, firewall, 413
Link encryption, 123
Local area networks (LANs), 411, 425
Logical link control (LLC) layer, IEEE 816, 233
Logic bomb, 356

M

MAC protocol data unit (MPDU), IEEE 816, 232–233, 235, 241–242
Macro viruses, 346–347
MAC service data unit (MSDU), IEEE 816, 232–234
Mail (DKIM), 289–295
  e-mail threats, 290–291
  functional flow, 292–295
  Internet mail architecture, 254–258
  strategy, 291–292
Mail Submission Agent (MSA), 255–256
Malicious association, 224
Malicious insiders, 177
Malicious software or malware
  attack kits, 340
  attack sources, 340–341
  classification of, 339–340
  terminology, 339
  types, 338–341
Malware countermeasure approaches
  detection, 361–362
  generality, 361
  global and local coverage, 361
  identification, 361
  minimal denial-of-service costs, 361
  removal, 361
  resiliency, 361
  timeliness, 361
  transparency, 361
Man-in-the-middle attack, 107–108, 199, 224
Manipulating online polls/games, 357
Markov process, 386. *See also* Statistical anomaly detection
Masquerade, 27
Masquerader, intruders, 376
Master secret creation, 202
Master session key (MSK), IEEE 802.11i, 246
Measured service, 172
Media access control (MAC) layer, IEEE 816, 232–233
Media gateway, 162
Memory sticks, 227
Message authentication, 78–112
  approaches to, 79–84
  code (MAC), 81–82, 93–95
  digital signatures, 109–112
  encryption, and, 80–81
  hash functions, 82–91
  introduction to, 79
  key distribution, 137–139
  one-way hash functions, 82–84
  public-key cryptography, 96–109
  secure hash functions, 84–91
  technique, 95–96
  TLS, 190, 192–194
Message authentication codes (MAC), 114, 193, 211
Message authentication key distribution, 137–139
Message Handling Service (MHS), 254
Messages, 26, 27, 30, 45–73, 79–84, 136, 277–278, 331–332. *See also* Encryption*;* Public-key cryptography
  attacks on, types of, 49
  authentication, 78–112
  byte ordering, 134
  confidentiality, 45–73
  modification of, 30
  pretty good privacy (PGP), 279–280
  release of contents, 25
  Secure/Multipurpose Internet Mail Extension (S/MIME), 268–279
  SSH exchange, 214–215
Message User Agents (MUA), 254, 255
Metamorphic virus, 346
Misfeasor, intruders, 377
Mix columns, AES, 57
Mobile code, 352
Mobile device security, 226–230
  cloud-based applications, 226
  de-perimeterization, 227
  elements, 229
  external business requirements, 227
  growing use of new devices, 226
  strategy
    barrier security, 230
    device security, 228–229
    traffic security, 230
    VPNs, 230
  threats
    applications by unknown parties, 228
    interaction with systems, 228
    location services, 228
    physical security controls, 227
    untrusted mobile devices, 227
    untrusted networks, 228
Mobility, 223
Model for network security, 39–42
Modification of messages, 27, 30
Modularity, 35
Morris worm, 350–351
Multipartite virus, 346
Multipurpose Internet Mail Extensions (MIME), 259–266
  canonical form, 264
  content types, 261–263
  transfer encodings, 263–266
Mutation engine, 346

N

National Institute of Standards and Technology (NIST), 42, 52, 87, 108
Native audit records, 383
Network access control (NAC)
  access requestor (AR), 161
    supplicants, 161
  context, 162
  enforcement methods
    DHCP management, 164
    firewall, 164
    IEEE 802.1X, 163
    VLANs, 163
  NAS
    media gateway, 162
    policy server, 161
    RAS, 162
  policy server, 161
Network access server (NAS), 162
Network activity, 413
Network attack surface, 36
Network injection, 225
Network security, 17–42, 119–155, 184–185, 222–250
  applications, 138
  authentication, 119–155
  computer security, 18
  defined, 18
  HTTPS, 188, 207–208
  information security, 18
  International Telecommunication Union (ITU), 24
  Internet Engineering Task Force (IETF), 42
  internet security, 19
  Internet standards, 42
  introduction to, 17–42
  mechanisms, 21–24, 32
  model for, 39–42
  open systems interconnection (OSI) architecture, 24–25
  Secure Shell (SSH), 208–219
  Secure Sockets Layer (SSL), 190–191
  services, 25, 29–32
  threats, 43, 177
  transport-level, 187–219
  violations of, 3 wireless, 222–250
  X.800 standard recommendations, 24, 27–28, 31–32
Nonce, 95, 328, 332
  Kerberos, 136
Nonrepudiation, 28, 30
Nontraditional networks, 224

O

Oakley Key Determination Protocol, 325
On-demand self-service, 172
One-way function, 379. *See also* Intrusion techniques
  authentication, 82–84
  hash functions, 82–84
Open design, 34
Open systems interconnection (OSI), 24–25
Options, Kerberos, 136

P

Packet exchange, SSH, 210–213
Packet filtering firewall, 414–418
Packets, IPsec, 312–314
Padding, 194, 315
Pairwise master key (PMK), IEEE 802.11i, 246–247
Pairwise transient key (PTK), IEEE 802.11i, 246–247
Passive attacks, security, 25–27
Password attacks, Kerberos, 135–136
Password cracking approaches, 400
Password management, Intruders
  bloom filter, 404–406
  hashed passwords, use of, 397–400
  selection strategies, 403–404
  user choices, 400–403
  vulnerability of, 396–397
Payload(s), 338
  attack agent
    remote control facility, 357
    uses of bots (*see* Bots, uses of)
    Zombie, 356
  classification-based worm containment, 365
  information theft
    credential theft, 358, 359
    identity theft, 359
    keylogger, 358
    phishing and identity theft, 358–359
    reconnaissance and espionage, 359
    spyware, 358
  stealthing
    backdoor (trapdoor), 359
    rootkit, 359–360
  system corruption, 355–356
    logic bomb, 356
    ransomware, 355
    real-world damage, 355–356
    Stuxnet worm, 356
Peer entity authentication, 29
Peer-to-peer networks, 224
Permanent key, defined, 123
Personal firewall, 422–423
Personal network Bluetooth devices, 224
Phishing and identity theft
  phishing attack, 358
  spear-phishing attack, 358
Physical layer, IEEE 816, 231
Physical security controls, lack of, 227–228
Plaintext, 48–50, 97
  chosen, attack, 49
  defined, 48
  known, attack, 48–49
  public-key encryption, 96
Platform as a service (PaaS), 173
Policy server, 161
Polymorphic virus, 346
Port forwarding, SSH, 217–219
Pre-shared key (PSK), IEEE 802.11i, 246
Pretty good privacy (PGP), 279–280
Private cloud, 173

Private keys, 145–146, 270–271, 279
  pretty good privacy (PGP), 279–280
  public-key cryptography and, 99–100
  usage, X.509 authentication service, 145
Proactive password checker, 403–404
Propagating cipher block chaining (PCBC) encryption, 135
Propagation
  infected content
    macro viruses, 346–347
    nature of viruses, 342–345
    scripting viruses, 346–347
    viruses classification, 345–346
  mobile code, 352
  Morris worm, 350–351
  remote execution capability, 348
  remote file access or transfer capability, 348
  remote login capability, 348
  social engineering
    spam (unsolicited bulk) e-mail, 353–354
    Trojan horses, 354–355
  state of worm technology, 351–352
  target discovery, 348–349
  vulnerability exploit
    client-side vulnerabilities, 352–353
    drive-by-downloads, 352
    electronic mail or instant messenger facility, 348
    file sharing, 348
  worm propagation model, 349–350
Protected data transfer phase, IEEE 802.11i, 239, 248–249
Protocol
  Diffie–Hellman, 104–105
  key exchange, 104–105
  PKIX management, 148–149
Pseudorandom function (PRF), 62, 203–204, 249–250
  IEEE 802.11i, 249–250
  IKEv2, 334–335
  TLS, 203–204
Psychological acceptability, 34
Public cloud, 173
Public-key cryptography, 96–109
  algorithms, 96–109
  applications for, 99–100
  ciphertext, 97
  cryptography, 96–109
  decryption algorithm, 97
  Diffie–Hellman key exchange, 104–107
  Digital Signature Standard (DSS), 108
  elliptic curve (ECC), 109
  encryption algorithm, 105–107
  encryption structure, 97–99
  plaintext, 97
  private keys, 97, 99
  public keys, 97, 99
  requirements for, 100
  RSA public-key encryption, 101–104
  secret keys, 99
Public-key encryption, 96–109
  algorithm, 46
  digital signatures, 108
  structure, 96–109
Public-key infrastructure (PKI), 146–149
  certification authority (CA), 147
  CRL issuer, 148
  end entity, 147
  key pairs, 148
  model, 146–149
  PKIX management functions, 148
  PKIX management protocols, 149
  registration authority (RA), 147–148
  repository, 148
Public keys, 97, 99, 140, 145
  authority key identifier, 145
  certificates, 138–139, 145
  cryptography, 97, 99
  defined, 99
  distribution, 137–138
  revoking, 146
  secret keys, distribution of using, 138–139
  subject key identifier, 145
  usage, X.509 authentication service, 147

Q

Quick Response (QR) code, 228
Quoted-printable transfer encoding, 264

R

Ransomware, 355
Rapid elasticity, 172
Rate halting, 366
Rate limiting, 366
RC4 algorithm, 65–67
  generation, 66
  initialization of S, 65–66
  logic, 66
  strength of, 66–67
Reactive password checking strategy, 403
Realm, 124–137
  concept of, 134
  Kerberos version 4, 125–134
  Kerberos version 5, 134–137
Real-world damage, 355–356
Reconnaissance and espionage, 359
  credential theft, 359
  identity theft, 359
Record Protocol, 191–194
Registration authority (RA), PKI, 147–148
Release of message contents, 25
Relying party (RP), 122
Remote access server (RAS), 162
Remote Authentication Dial-In User Service (RADIUS), 166
Remote execution capability, 368
Remote file access or transfer capability, 348
Remote login capability, 348
Replay, 27
Replay attacks, 126
Repository, PKI, 138
Request for Comment (RFC) standards, 25, 259, 290–291
  RFC 4686, e-mail threats, 290–291
  RFC 5322, S/MIME, 268–269
  security recommendations, 24

Resource pooling, 172–173
Resources, 223
Response, IDES, 395
Reverse certificate, 143
Revocation, 144, 148
  certificates, X.509 authentication service, 143
  request, PKI, 148
Rivest-Shamir-Adleman (RSA) algorithm, 199–202
Rootkit
  countermeasures, 364
  external mode, 360
  kernel mode, 360
  memory based, 360
  persistent, 360
  user mode, 360
  virtual machine based, 360
Round
  Add Round Key, 57
  AES encryption, 59
  function, Feistel cipher, 50–52
Routing, IPsec, 306
RSA, 101–104
  public-key encryption, 101–104
RSA probabilistic signature scheme (RSA-PSS), 111
Rule-based anomaly detection, 386
Rule-based detection, 382
Rule-based intrusion detection, 386–388
Rule-based penetration identification, 387–388

S

Salt value, 397. *See also* Hashed passwords
Screening router, 428
Scripting viruses, 346–347
Second-generation scanner, 362
Secret keys, 46, 99, 138–139
  encryption using, 46
  key management, 138–139
  public-key cryptography, 99, 138–139
  public-key distribution of, 138–139
Secure Hash Algorithm (SHA), 87
Secure hash functions. *See* Hash functions
Secure/Multipurpose Internet Mail Extension (S/MIME), 268–279
  certificate processing, 278–279
  clear signing, 277
  cryptographic algorithms, 273–274
  messages, 274–278
  Multipurpose Internet Mail Extensions (MIME), 259–266
Secure Shell (SSH), 208–219
  channels, 216
  Connection Protocol, 209
  host keys, 209–210
  key exchange and generation, 213–214
  message exchange, 214–215
  packet exchange, 210–213
  port forwarding, 217–219
  Transport Layer Protocol, 209–213
  User Authentication Protocol, 209, 214
Secure Sockets Layer (SSL), 190
Securing wireless transmissions, 225–226
Security as a service (SecaaS), 182
Security assessments, 184
Security association database (SAD), 310–311
Security association (SA), IP, 309–310, 322–325
Security attacks, 25–27
  active, 27
  defined, 25
  denial of service, 27
  masquerade, 27
  modification of messages, 27, 30
  passive, 25–27
  release of message contents, 25
  replay, 27
  traffic analysis, 26
Security design principles, 32–36
Security information and event management (SIEM), 184
Security mechanisms, 23–24, 31–32
  services and, relationship of, 32
  X.800 recommendations, 31
Security policy, 395
Security policy database (SPD), 311–312
Security policy violation, 39
Security services
  access control, 29
  authentication, 29
  availability, 30
  data confidentiality, 29
  data integrity, 28, 30
  defined, 25, 30
  nonrepudiation, 30
Sender policy framework (SPF), 267, 286–289
  mechanism modifiers, 288
  operation, 289
  on receiver side, 288–289
  on sender side, 288
Separation of privilege, 34
Sequence number, 137
Service models, 173
Service request, SSH, 213
Service set identifier (SSID) broadcasting, 225
Service threats, defined, 41
Session keys, 60, 123, 135
  defined, 60, 123
  Kerberos, 135
Shared technology issues, 177–178
Shift rows, AES, 56
Signal-hiding techniques, 225
Signature detection, 382. *See* Rule-based detection
SignedData, S/MIME, 276–277
Simple Mail Transfer Protocol (SMTP), 415–416, 418
Single bastion inline, 424, 428
Single bastion T, 428
Small office/home office (SOHO) applications., 428
Smartphones, 227
SMTP, 415–416, 418
SOCKS, components, 420
Software as a service (SaaS), 173
Software attack surface, 36
Source routing attacks, 417
SSL/TLS attacks, 205–207
Stanford Research Institute (SRI), 386