| A | abstractions, 15, 61, 63, 429, 435, 626 |
|   | abstract network security credentials, 519 |
|   | abstract relationship, between network target and attacker, 518 |
|   | academic/professional credentials, 3 |
|   | acceptance testing, 37, 654 |
|   | access border control function (A-BCF), 598 |
|   | access control concepts, 244, 245 |
|   | access control devices, 13 |
|   | access control entries (ACEs), 479 |
|   | specified trustees and information, 481 |
|   | steps describe preferred order of, 481 |
|   | access control list (ACL), 9, 478, 479 |
|   | components, 478 |
|   | model, 14 |
|   | access control scenario, 245 |
|   | active subjects accessing, 245 |
|   | alter mode, 245 |
|   | append mode, 245 |
|   | discretionary access control, 246 |
|   | execute access, 245 |
|   | mandatory access control, 246 |
|   | observe mode, 245 |
|   | passive objects, 245 |
|   | read/write mode, 245 |
|   | specific access operations, 245 |
|   | write access mode, 245 |
|   | access control systems and methodology, 8 |
|   | access masks, 481 |
|   | access networks, 372 |
|   | functions, 382 |
|   | access rights, 481 |
|   | generic/standard, constants, 482 |
|   | and mask, 481 |
|   | access service networks (ASNs), 295 |
|   | access service providers (ASPs), 52 |
|   | access-technology dependent functions, 382 |
|   | access tokens, 478 |
|   | accounting management activities, 634 |
|   | accreditation, 14, 658 |
|   | ACEs, see access control entries (ACEs) |
|   | acquisition costs, 36 |
|   | activation services, securing management, 638 |
|   | active directory (AD), 362, 363, 487 |
|   | domain services support, inheritance of, 492 |
|   | features, 487–489 |
|   | network components, logical structures for, 489 |
|   | objects, 490 |
|   | access control for, 492 |
|   | using domain name service, 489 |
|   | domain forest, 490 |
|   | domain tree, 489 |
|   | transitive trusts in a domain forest, 491 |
|   | in Windows Server 2003, 488 |
|   | active optical networking, 309 |
|   | AD. see active directory (AD) |
|   | address ranges, and default sub-net mask by address class, 323 |
|   | address resolution protocol, 310 |
|   | ad hoc network, 616 |
|   | administration, 4, 9, 37, 64, 223, 404, 473, 644, 669 |
|   | administrative account management, 648 |
administrative personnel controls, 13
administrative tasks, in access control methods, 248
groups and permissions, 248, 249
protection rings, 249, 250
administrators, 15, 241, 492, 622, 629
advanced encryption standard (AES) encryption algorithm, 309
AH. see authentication header (AH)
air conditioning, 13
airport security checks, 2
Akamai Technologies Inc., 25
Alliance for Telecommunications Industry Solutions (ATIS), 259, 262
committees, 262
American Express, 49
American National Standards Institute (ANSI), 259
analog–ISDN local loops, 283
ANSI/ATIS 0300074.2006, 681
anti-malware applications, 512
host-based firewalls, 513–514
host-based intrusion detection, 515
malware and spyware scanners, 512–513
modification scanners, 514–515
antivirus, 13
Apple’s MAC OS-X product, 662
application and systems development security, 9
application functional group (FG), 381
applications border control function (AP-BCF), 598
application security issues, 498
application development security, 501
automated code reviews, 502
code security reviews, 501
files and stages from implementation to execution, 501
manual code reviews, 502
bounds checking, 500
buffer overflow problems, 499, 500
dynamic code security analysis, 503
exception handling, 500
shared libraries, 500
static code security analysis, 502
applications, securing management framework, 645–648
administrative account management, 648
authentication credentials management, 648
ITU-T Recommendation M.3410, 646
security configuration management, 647–648
security event, fault, and attack management, 647
TMN System Security Management, 645
verification/validation management, 648
management of, 642
element management systems (EMSs) security needs, 643
NMS security additions, 644
selected OSS/EMS security services, 644–645
management roots, 633, 634
operation/administration/maintenance/decommissioning, 648
operational security compliance Program, 664
element security tools, 667–669
penetration testing, 669–671
security compliance report, monitor, and improvement, 667
operational security mechanisms, 649
acceptance testing/field testing/operational readiness, 653–654
accountability, 653
documentation, 653
duties/roles, separation, 649–650
guidelines/procedures, 650–651
human resources/legal aspects, 653
independent auditing/review, 651–653
operations security, 654
accreditation/certification, 658–661
life-cycle review, 661
reviews, 657–658
security event response/forensics, 655–657
senior security management mechanisms, 657
third-party access, 655
withdrawal from service, 661–663
systems implementation/procurement, 671–681
acceptance testing and review, 681
forensic tools, 681
requests for information/proposals (RFIs/RFPs), 673–679
standards compliance, 679–681
telecommunications management
network, 634
element/network management systems/
operations systems, 636–640
security, 640–642
structure, 635–636
applied cryptography, 81
architectural models, 14
architecture evaluation methodologies, 14
ARP (Address Resolution Protocol)
spooﬁng, 275, 310
announcements, 313
attacks, 315
MitM, 316, 317
cache values, 315–318
defenses against gratuitous ARP-based
attacks, 319, 320
gratuitous ARP broadcast by, 316, 318,
319
messages, 313
format, 314
MitM for packets, being sent, 317
normal packet ﬂow, 315, 317
Probe, 314
vulnerabilities and attacks, 314
assess performance, 38
asset inventory, and classiﬁcation, 201
conceptual assets, 202
logical assets, 202
physical assets, 201, 202
assets, 26, 169
protection, 25
vulnerabilities, 204
asymmetric encryption algorithms, 11, 93
bit error propagation examples, 95
CBC error propagation, 96
performance, 95
using private key, 93
using public key, 94
asynchronous transfer mode (ATM), 304
ATM header, 309
auditing, 11, 12, 13, 66, 77, 206, 252, 493,
650, 660, 667
audit trails, 13
authentication, 14
authentication, authorization and accounting
( triple A ) servers, 295
authentication credentials management, 648
authentication systems, 123
Kerberos-based authentication, 124
limitations of KDC-based protocol, 128
rationale for developing, 124
security-related servers, 124
Kerberos message exchanges, 127
Kerberos terms and deﬁnitions, 125
authenticity, 11, 65, 85, 153, 181, 300, 340,
370, 591, 637
automatic tunneling, 332
availability, 8, 11, 14, 26, 62
chassis, 650
protection, 204, 222
vulnerabilities, 209
B
backdoors, 507, 509
bankruptcy, 26
basic input–output systems (BIOS), 451
desirable BIOS platform hardware
security-related mechanisms, 456
hardware mechanisms, 451
software mechanisms, 451
Bell–LaPadula (BLP) security model, 14,
253, 254
Biba integrity model, 14, 256
billing, securing management, 639
biometrics, 423
technologies, 155
BIOS. see basic input–output systems (BIOS)
Black box, 665
blackmailing, 19
“Bluetooth” wireless devices, 300
Border Gateway Protocol version 4
(BGPv4), 352
Boston Globe, reports for cybercrime, 25
botnets, 510, 511
bounds checks, 673
broadband connection, 22
broadband passive optical network (BPON)
home network, 308
broadband wireless access, 295
“buffer overﬂow,” 19
business continuity plan, 10
development, 10
business impact assessment, 10
business management layer (BML), 396, 635
business/organizational types, 52–53
  commercial, 53
  government, 54–56
  unit abbreviations, 55
  nongovernmental organizations, 56
  residential, 54
  applications range, 54
business risks, 671
business workflow, securing management, 637

C
cables, 3
  modems, 385
Cable Television Laboratories, Inc.
  (CableLabs), 262
capability maturity model (CMM), 41, 43–46
  conscious competence, 44
  conscious incompetence, 43
  key process areas (KPAs), 44
  features, 44
  goals of, 44
  levels, 44–46
  process improvement approach, 41
  unconscious competence, 43
  unconscious incompetence, 43
  usage, 44
capability maturity model for software
  (SW-CMM), 46
capability maturity model integration
  (CMMI), 46
  models, 46
  Product Team’s mission, 46
  Version 1.2 Product Suite, 46
CBK Cryptography domain, 11
  CC. see common criteria (CC)
CDMA2000 1x (TIA IS-2000) digital cellular technology, 100
cellular networks, 294, 295
  code division multiple access
  (CDMA), 294, 382
  global system for mobile communications
  (GSM), 294
  universal mobile telecommunications system (UMTS), 294
Center for Internet Security (CIS)–Benchmark Tools, 666
central processing unit (CPU), 411
cipher proposal acceptance (CPA), 539
Circuit switched networks, 279
  bandwidth, 280
  call and circuit path, 285
  connection type, 280
  connects, 280
  framing, 280
  media, 280
  PSTN switch hierarchy and parallel signaling system, 286
  signaling, 280
  Signaling Protocol SS7, 285
CISP Corp., 15
  Citicorp’s electronic funds transfer system, 20
civil laws, 11
Clark–Wilson model, 14, 256–258
Clark-Wilson security model, 649
Clark-Wilson Trusted Process (TP), 649
clouds, 289
  applications as a service, 292, 293
  hardware as a service, 290, 291
  infrastructure as a service, 291, 292
  public vs. private clouds, 293
CMM. see capability maturity model (CMM)
CMMI for Development (CMMI-DEV), 46
code of conduct, 11
combined voice and text instant messaging, 51
commercial enterprises, 52
commercial off-the-shelf (COTS) technologies, 51
common body of knowledge (CBK) security domains, 8
common criteria (CC), 14
contents, 228
mitigation approach, 227
security concepts and terminology, 228
common network devices, 14
Common Object Request Broker Architecture (CORBA), 264, 428, 590, 624, 626, 637
element types, 625
security space, 625
communications, 23
management networking, 635
networks, 14
communications management information protocol (CMIP), 212, 634
competition, 47
via information services, 51
competitive local exchange carrier (CLEC), 637, 639
competitive local exchange carriers (CLEXs), 52
compiler, 63, 621
compliance, 8, 11, 13, 38, 170, 183, 186, 648, 665–667, 671. see also operations compliance
cycle major phases, 664
verification process, 665
computer-based applications, 23
crime laws, and regulations, 11
crime response team (CERT), 653, 657
crime forensics, 12
crime forensic tool testing (CFTT) project, 657, 681
crime hijacking, 21
reasons, 21–22
crime security, 1, 4, 21, 24
central role of, 1
crime security incident management, 655
Computer Security Institute (CSI), 20
crime-to-computer communication, 522
crime equipment hardware, 4
crime concept of integrity, 65
data integrity, 65
defined as, 65, 66
information integrity, 65
origin integrity, 65
crime concept of “security” domain, 61
crime confidentiality, 8, 11, 14, 62, 70, 197, 253, 308, 342, 368, 450, 546, 593, 662 of data, 645
confidentiality, integrity, and availability (CIA), 8, 53, 54, 58, 65
crime-oriented security models, 252
commercial setting, 252
crime policies, 252
configuration management activities, 634
configured tunneling, 332
connectionless networking
example initial routing tables, 313
within internetworking layer, 313
router B routing table change, 314
connectivity service network (CSN), 295
control objectives for information and related technology (COBIT), 189–194
COBIT 4.1, 189
COBIT 5, 189
convenience, 2
CORBA web services, 636, 637
core border control function (C-BCF), 598
core/services network, 376
core transport functions, 383
corporate organization structure, 651
cost–benefit analyses, 31
cost–benefit trade-off, 35
cost-effective information security, 2
CPE WAN Management Protocol (CWMP), 367
credit cards, 49, 155
companies, 17, 25
criminal organizations, 24
critical infrastructure protection (CIP) plan, 57
defines sector and organizational responsibilities in a standard, 57, 58
cryptanalysis, 101–104
cryptographic algorithms, 104
data encryption algorithm (DES), 103
encryption times
relation of key length to, 103
Kerberos authentication scheme assigns DES keys, 104
key protection, 106, 107
key randomness, 106
one-time pad (OTP) scheme, 102
processor ability to try a complete key space, 105
recognizable plain-text, 104
securing against cipher-text, 104
typical instruction execution rates
cryptanalysis (Continued)
for commercially available processors, 104
using passphrases with cryptography, 108
using passwords with cryptography, 107, 108
cryptographic authentication, 112, 113
challenge–response technique, 113–116
data integrity, 112
data-origin, 112
digital signature authentication
technique, 119, 120
message authentication code
technique, 116–118
cryptographic hash approach, 116, 117
symmetric encryption approach, 117, 118
of messages, 113
peereentity, 112
primary approaches to authentication, 113
provide protection against active attacks, 113
strong, 113
unilateral (one-way) or mutual (two-way), 113
cryptographic hash algorithm
attributes, 81–82
currently available, 83
generic, 82
prevalent hash functions, 82
role in information security, 83
cryptography, 10, 11, 61
role in information security, 77
CSI. see Computer Security Institute (CSI)
customer domain, 374
customer edge-access routers, 283
customer edge routers (CERs), 301, 302, 377–379, 552, 553
customers, protection of, 62
compliance, 62
confidentiality, 62
integrity, 62
interaction
error-free and non-malicious, 62
cyber attacks, 52
cyber-blackmail, 24
cybercrime, 23, 24, 47, 52, 59
cyber-security, 24
cyberspace, 1
cyberwarfare, 23, 24
component of international conflict, 24
D
database-oriented requirements tracking
systems, 35
data classification, 11
data communications, 634
datagram transport layer security
(DTLS), 342, 367, 574–581
record protocol operation, 580
data integrity, 65, 66, 141, 349, 351, 443, 545
data link, 14, 270, 296, 331, 377, 524, 597
layer, 524
protocols, and security capabilities, 312
data link layer protocols security, 310
data local exchange carrier (DLEC), 637, 639
companies, 637
data security standard, 49
debit cards, 155
decommissioning, 648, 649
decryption, 11, 88
algorithm, 81
Defense Information Systems Agency
(DISDA), 198
defensive controls, 5
demilitarized zone (DMZ), 518
denial-of-service (DoS), 640
attacks, 404
DenyHosts, 668
design engineers, 35
destroy information, 11
detection, 5, 7, 99, 340, 450, 506, 518, 630, 645, 648
deterrent controls, 4, 5
devices, in processing SIP VoIP calls, 598
DHCP. see dynamic host configuration
protocol (DHCP)
“dialback” modems, 522
diameter, 149
compatible with RADIUS, 149
defined by RFC 3588, 149
Diffie–Hellman (DH) value, 539
digest algorithms, 607
digital rights management (DRM), 51
digital signature algorithm (DSA), 83, 95
digital signature based MAC data
integrity, 86
digital subscriber line (DSL), 304
access network, 305
in-home connections, 305
RJ-45 interface/RJ-11 interface, 304
Digital Subscriber Line (xDSL) technology, 382, 385
digital time division multiplexed (TDM) circuit, 279
disaster recovery plan, 10
discretionary access control (DAC), 9, 246
using an access control list approach, 246, 247
discretionary access control list (DACL), 478, 479
access control with, 480
distributed computing environment (DCE), 344, 444, 626–630, 627, 636
architectural components, 629
cell characteristics, 627
cell components, 627, 628
layered mode, 628
security protocol, 628
Security Services are based, 628
document disciplinary activities, 3
domain name system (DNS), 351, 359, 360
cache poisoning, 360
DNS security (DNSSEC), 361
domain name spoofing, 361
security extensions, 605, 606
server compromise, 360
servers, 357
domain namesystem (DNS) security extensions (DNSSEC), 605
domains, 64
perspective, 373
and trust relationships, 485–487
DTLS. see datagram transport layer security (DTLS)
dynamic host configuration protocol (DHCP), 355, 630
assigned IP addresses, 358
Option 90 authentication information, 630
password authentication message, 631
server, 357
techniques for authentication, 630
vulnerability, 358

E
EAP. see extensible authentication protocol (EAP)
EC. see elliptic curve (EC)
ECC. see elliptic curve cryptography (ECC)
EC-Council, 670
device functions, 383
electrically reprogrammable memory (EEPROM), 157
element management layer (EML), 396
systems, 396, 397
element management systems (EMSs), 636, 643
element security architecture
description, 426–429
generic view, 427
kernel, 429, 430
security contexts, 430–432
security-critical functions, 432
audit function, 433, 434
authentication function, 433
device management functions and device controllers, 434, 435
process scheduling function, 434
security policy decision function, 432, 433
security-related functions, 435
ElGamal encryption system, 94
elliptic curve (EC), 83
elliptic curve cryptography (ECC), 95, 99, 100
redundant data, 99
e-mails, 24, 25, 376, 583
attacks, 587–589
embedded (“real-time”) operating systems, 449
desirable embedded OS platform hardware security-related mechanisms, 450
embedded OS context security-related software functions, 452–455
hardware mechanisms for embedded OS usage, 449, 451
software mechanisms for embedded OS usage, 451
embedded OSs, 496–498
control, 498
emergency procedures, 13
employment, 3, 52, 176–178
pre and post, 13
encapsulating security payload (ESP), 332, 536
encrypted data, 11
encryption algorithms, 81, 86
irreversible transformations, 81
performance, 95
automatic repeat-request (ARQ), 99
BER by media type, 100
BIT error propagation, 95
CBC error propagation example, 96
communications bit errors by media
type, 97
detecting errors, 99
encryption algorithm speed, 100
forward error correction (FEC), 99
processing times for AES encryption/
decryption, 101
stream error propagation example, 98
transmission BER, 97
reversible transformations, 81
enforcement, 8, 62, 163, 418, 432, 626
ingenreering process, for complex systems, 39
enhanced Telecom Operations Map®, 397
Enron, 46
Enterprise information security program, 199
Enterprise role model, 390–392
Enterprise security governance, 664
Enterprise security policies, 189
environmental and life safety controls, 13
ESP. see encapsulating security payload (ESP)
ethernet, 297
ethernet, 297
-frame and header, 298
MAC addresses, 314
protocol layering over, 299
virtual ethernets, 299, 300
VLAN-tagged Ethernet frame, 300
ethical issues, 11
eTOM
decompositions of processes, 401
framework, 398, 401
horizontal views, 401
major process areas, 399
operations support and readiness (OSR)
forms, 401
strategy, infrastructure, and product (SIP)
process area, 401
structure of functions, 400
ETSI security-related vulnerability, and threat
analysis efforts, 230
ETSI ES 202 382, 231
ETSI ES 202 383, 231
ETSI Guide 202 387, 230
TS 102 556, 231
European Telecommunications Standards
Institute (ETSI), 259, 263, 295,
385
standards, 230
ex–black-hat hackers, 670
excel spreadsheets, 35
exception handling, 672
extensible authentication protocol (EAP),
145
architecture, 146
authentication methods, 147
defined in RFC 5247, 146
EAP-AKA, 148
EAP-IKEv2, 147
EAP-IKEv2 credential combinations, 148
EAP-LEAP, 148
EAP-logoff message, 524
EAP-PEAP, 149
EAP-PSK, 148
EAP-Request identity message, 524
EAP-SIM, 148
EAP-TLS, 147
EAP-TTLS, 148
methods capable of operating in wireless
networks, 146
methods, defined in IETF RFCs, 146
vendor RADIUS and EAP support, 149
eXtensible Markup Language (XML), 348,
349
security, 589

F
facility control requirements, 13
facility security management, 13
fast frequency hopping, 523
fault management services, 634, 639
faults, configuration, accounting, performance,
and security (FCAPS), 634
fault tolerance technologies, 13
FCAPS messages, 376
FDIC-insured institutions, 24
Federal Communications Commission
(FCC), 260
Federal Information Processing Standards
(FIPS), 196, 197
Federal Information Security Management Act
(FISMA), 196–199
NIST establishing FISMA Implementation Project, standards and guidelines, 196
FIPS Publication 199, 196
FIPS Publication 200, 197
NIST Special Publication (SP) 800-53, 197
SP 800-37, 197
SP 800-39, 197
SP 800-59, 197
SP 800-60, 197
SP 800-53A, 197
risk management framework, 198
fence protection mechanism, 413
memory fence register, 413
field testing, 654
finance, 23, 53, 64, 655
financial institutions, 21
fire detection, 13
forensic investigators, 656
forensic tools, 681
frame relay (FR), 304
framework, of NGN functional reference model, 380
fully qualified domain name (FQDN), 359, 552
functional elements (FEs), 36
functional entities (FEs), 372
functional groups (FGs), 372, 373
of elements, 36
functional planes, 376, 377

G
gateway functions, 383
general application protocols security, 350
general network security architectures, 401, 402
generic attack, 225
derial of service, 225
masquerade, 225
outsider attacks, 225
replay, 225
trapdoor, 225
trojan horse, 225
generic stream encryption, 89
generic symmetric encryption, 87
stream encryption, 88
generic threat objectives, 220

Global Information Assurance Certification (GIAC), 671
global positioning system (GPS), 640
government agencies, 21
Graham–Denning confidentiality model, 254, 255
graphical user interface, 637
group temporal key (GTK), 529

H
Hamming codes, 99
hardware, 2, 410
cryptographic mechanisms, 411
protecting software, 410, 411
security-related capabilities, 410
hardware encryption, 421
hardware acceleration cards, 422
hardware acceleration USB devices, 422
hardware security modules, 421, 422
Smartcards, 423, 424
hardware faults, 13
hash algorithms, 81
heating, 13
HMAC based MAC Data Integrity, 87
HMAC-MD5 authentication message, 632
HMAC-MD5-96 method, 83, 85
HMAC-SHA1-96 method, 83, 85, 86
Home Location Register (HLR) central servers, 294
home network mobility agent (HA) functionality, 354
home subscriber server (HSS), 386
human authentication, 154–155
biometric authentication, 154, 155
characteristics, 154
factors, 154
automatic teller machine (ATM), 157
combination of, 157
online (“web”) access, 157
remote access, 157
three-factor authentication, 158
two-factor authentication, 157
passphrases, 156
password changing policies/requirements, 155
password vulnerability, minimized by, 154
proxies for humans, 159
operating systems, 159
single sign-on (SSO), 159–161, 164
human authentication (Continued)

  user agents, 159
  rainbow tables, 158
  required attributes for quality passwords, 156
  Smart cards, 154
  subject
    knowing factor, 155–156
    location of factor, 157
    possess factor, 155

human resources (HR), 653
hypertext markup language (HTML), 589
hypertext transfer protocol (HTTP), 344, 589, 593
  Base64 algorithm, 345
  basic authentication scheme, 344
  digest access authentication, 345
  cookies and other security issues, 346
drawbacks, 345, 346
  security vulnerabilities or attacks, 347, 348

I
ICMPv4 message fields, 326
  within an IPv4 packet, 325
ICMPv4 message types, 326
identical ITU-T, and ISO security framework standards, 403
identity management (IdM), 164–167, 589
categories, 167
“identity theft,” 17
IEEE 802.16 wireless network, 295
illegal software, 13
illicit data, 25
IM. see instant messaging (IM)
import–export laws, 12
IMS enabled network
  core FGs within the services stratum, 385
    Application Servers (AS), 387
    Breakout Gateway Control Function (BGCF), 387
    Call Session Control Function (CSCF), 386
    Home Subscriber Server (HSS), 386
    I-CSCF (Interrogating-CSCF), 387
    Media Gateway (MGW), 387
    Media Resource Functions (MRFs), 387
    Proxy-CSCF (P-CSCF), 386
    Serving-CSCF (S-CSCF), 386
    Signaling Gateway (SGW), 387
IMS FE locations within an NGN, 388
incident planning, 12
incumbent local exchange carriers (ILEXs), 52
information assurance, 169
information breaches confidentiality, 11
information integrity, 65
  integrity policy principles, 66
  auditing, 66
  separation of duty, 66
  separation of function, 66
information resource protection, 220
  vulnerabilities, 206, 207
information security, 4, 14, 27, 169
  and risk management, 11
  role of cryptography in, 77, 81
information security systems engineering methodology, 199
  components within a security program and relationships, 200
  security life cycle, 200
Information Systems Audit and Control Association (ISACA), 189
  published documents, 189
  risk IT framework 2009, 189
information technology, 48
Information Technology Infrastructure Library (ITIL), 194–196
  activities
    control, 195
    evaluation, 196
    implementation, 195
    maintenance, 196
    plan, 195
ITIL Continual Service Improvement, 194
ITIL Service Design, 194
  address issues, 194
  ITIL Service Operation, 194
ITIL Service Strategy, 194
ITIL Service Transition, 194
  process deals/compliance with, 195
  primary goal, 195
  processes covered under service design, 194
  sub-activities and descriptions, 195, 196
Information Technology Security Evaluation Criteria (ITSEC), 14, 230, 659
InfoSec diagnosis and treatment, 28
infrastructure, protection
access to system attributes based on authorized, 62
confidentiality, 62
error-free and non-malicious interaction, 62
integrity, 62
initial internet user application protocols, 344
instant messaging (IM) and chat applications, 608
protocols, 609
specific attacks, 615
UA capabilities, 613–614
user agents (UAs), 610–612
Institute of Electrical and Electronics Engineers (IEEE), 259
Integrated Product Development Capability Maturity Model (IPD-CMM), 46
integration, 27, 29, 36, 39, 54, 55, 391, 499, 654, 673
integrity, 8, 11, 14 capabilities, 645
integrity policies, 252
formal definition of integrity, 253
principles of operation, 253
set of integrity requirements, 253
Intel 80386/80486 family of processors, 412
Interconnect Border Control Function (I-BCF), 598
interconnecting equipment, 4
Inter-exchange carriers (IXCs), 52
interface control document, 37
interfaces, 37, 374, 376, 377
interim evolution of TMN layers of management functionality, 399
intermediate
and end device security, 223
and end node vulnerabilities, 211, 212
internal NNI (INNI), 374, 376, 378
(inter-)national and regional corporations, 52
International Council on Systems Engineering, 32
International Information Systems Security Certification Consortium, 8
International Organization for Standardization, 263
International Standards Organization (ISO), 41, 259, 269
standards on process management, 41
International Telecommunications Union, Telecommunications Sector (ITU-T), 259, 262
Internet, 48
and backbone service providers, 280
communication, 279
Internet control management protocol (ICMP), 325
Internet Engineering Task Force (IETF), 259, 264
Internet key exchange (IKE), 532
Internet Key Exchange (IKE) protocol, 536
Internet network model, 272–274
application protocols used within Applications layer, 273
characteristics of Internet layers, 272–273
protocols, used for communications, 273
Internet Protocol (IP), 279
headers, 274
between systems, 273
Internet Protocol version 4 (IPv4), 320
header, 320
Internet service providers (ISPs), 144, 274
Internet technologies, 1
Internetworking layer protocols, 310
and security capabilities, 333
internetworking layer protocols security, 332
Intersecurity domain communications, 428
Inter-SP interconnection, 382
Intranet, 277
intrusion detection and alarms, 13
inventory control, 13
investigations, 8, 11, 662
IP addresses, 9
IP-based network, 357
IP internetworking protocol, 310
IP multimedia subsystem (IMS), 385
IP packet authorization, and access control, 558
application-level gateways, 564, 566, 567
deep-packet inspection (DPI), 567–570
demilitarized zone (DMZ), 563–564
semi-trusted, 564
filtering rule, 561–562
intrusion detection system (IDS) placement, 569
intrusion prevention system (IPS) placement, 570
IP packet authorization, and access control
(Continued)
IPS general functional components and operation, 570
network and host packet filtering, 559–563
packet-filtering process, 560
packet-filtering router, 563
screened single-homed bastion host system, 568
screened-subnet firewall system, 568
typical multiple router–firewall deployment, 565
IPS applications, 649
IPS deep-packet inspection rules, 651
IPsec. see IP security (IPsec)
IPsec tunnel mode encapsulation, 325
IP security (IPsec), 332, 643
capabilities, 332
IPTV Interoperability Forum (IIF), 262
IPv4 Address Conflict Detection (RFC 5227), 314
IPv4 addresses, 321, 322
ranges, 322
IPv6 Datagrams within IPv4 packets, direct encapsulation, 331
IP version 6, 329
header, 330
IPv4 fragmentation, and related attacks, 327, 328
overlapping fragment attack, 329
teardrop attack, 329
tiny fragment attack, 328
IPv4 header, 320
-based attacks, 324
IPv6 header fields, 330
IPv6 headers, sequence of, 331
IPv4/IPv6 header translation, 330
IPv6 network, 331
IPv6 optional extension headers, 331
IPv6-over-IPv4 tunneling mechanisms, 331
IPv4 packer header, 321
IPv6 packets, 325
IPv4 packet tunneled
within an IPv4 packet, 325
IPv4 transport protocol
port number, 323
IPv4 tunneling, 324
IRC Corp., 15
ISDN digital local loop framing, 283
ISO 7498-4, 633
ISO 9000, 660
ISO 9001, 657
ISO 27001, 185, 657
major sections of, 186, 187
ISO 27001/27002, 660
ISO 27002, 172
access controls (section 11), 180
asset classification and control (section 7), 175
business continuity management (section 14), 182
communications and operations management (section 10), 179
compliance (Section 15), 183, 184
establishing organizational security policy (section 5), 172, 173
information security incident management (section 13), 182
information systems acquisition, development, and maintenance (section 12), 181
major topics (clauses), covered by, 172
organizational security infrastructure (section 6), 173–175
personnel security (section 8), 176–178
physical and environmental security (section 9), 178
specific actions need to be performed, 172
ISO 9001 certification, 660
ISO/IEC 27000, 185
ISO/IEC 27002, 185
ISO/IEC 27003, 185
ISO/IEC 27004, 185
ISO/IEC 27005, 185
ISO/IEC 27006, 185
ISO/IEC 9000 standard, 659
ISO/IEC 14000 standard, 659
ISO/IEC 27001 standard, 659
ISO 9000 processes and procedures, 41, 42
ISO 9000 quality management systems, 42
ISO 9001 quality management systems, 42
ISO 9004 quality management systems, 42
ISO 9001:2008 standard, 43
IT audit and assurance guidelines, 192, 193
IT audit and assurance standards, 192
IT audit and assurance tools and techniques, 193, 194
ITIL. see Information Technology Infrastructure Library (ITIL)
ITU Telecommunication Standardization Sector, 263, 264
ITU-T recommendation M.3410, 681
ITU-T recommendations X.805, 679
ITU-T X.700, 633
ITU-T X.805 approach to security, 403–405 security planes, 404
ITU-T X.800 generic architecture, 402
ITU-T X.800, security services definition, 69
ITU-T X.81x recommendations, 403
ITU-T Y.2012 functional architecture recommendation, 371

J
Java, 618
Java 2 cryptographic architecture, 620
Java Development Kit (JDK)
version 1.0, 618
version 1.1, 618
version 2.0, 618, 619
Java domain relationships, 620
Java security and cryptography, 621
Java security model, 618
sandbox concept, 618
Java 2 security model, 619
Java software programs, 618
JDK. see Java Development Kit (JDK)

K
kernel, 14, 428–430
key distribution centers (KDCs), 123, 126
Keyed digest based MAC Data Integrity, 84
key management, 108
addressing issues, 108
civilian re-keying schedules, 110
“dialogue” approach, 110
Diffie–Hellmann key distribution, 110–112 authentication, 111, 112
normal Diffie–Hellman exchange of messages, 111
exponential growth of secret keys, 110 revisited, 120
Diffie–Hellman exchange of messages attacked by MITM, 120
digital signature defense against the MITM attack, 121
secret key explosion, 109

L
label distribution protocol (LDP), 351 constraint-based, 351
LANs. see local area networks (LANs)
laptops, 21
launching system, 37
layer 2—data link security mechanisms, 524
10.8. 802.1AE modification to 802.3 ethernet frame, 527
802.11i, 528, 529
IEEE 802.1ae, 525–528
802.1x message flows, 526
IEEE 802.1ae SecTAG fields, 528
IEEE 802.11 WPA, 528, 529
IEEE 802.1x, 524, 525
layer 4—transport security protocols, 573 comparing characteristics of, 581, 582
datagram transport layer security (DTLS), 574–576
record protocol operation, 580
secure shell protocol (SSH), 581
secure sockets layer (SSL), 574–576
record protocol operation, 580
security items, 579
virtual private networks, 579, 581
transport layer security (TLS), 574–576
operational activities, 579
record protocol operation, 580
security items, 579
session establishment, 576–579
layer 5—user service application protocols, 582
email, 583
e-mail attacks, 587–589
pretty good privacy (PGP), 583–586
secure/multipurpose internet mail extensions (S/MIME), 586–587
S/MIME and OpenPGP differences, 587, 588
LDP. see label distribution protocol (LDP)
legal evidence, 12
best, 12
circumstantial, 12
conclusive, 12
direct, 12
expert opinion, 12
hearsay, 12
secondary, 12
legal issues, 11
legal liability, 47
legislation, 25, 28, 47, 49, 51, 165, 177, 236, 664
life-cycle costs, 35
lightweight directory access protocol (LDAP), 351, 361
Linux malware, 512
local area networks (LANs), 14, 274, 560
  broadcast, 275
  partitioned, 276
  point-to-point switched, 275
  typical wired LAN network segment, 276
VLAN soft partitioned, 276
local security authority (LSA), 477
Lockheed Martin Corp., 24
logging facility, 220
logic flaws, 14
logon procedures, 241, 242, 477
long-term evolution networks, 295
low-density parity-check (LDPC) codes, 99, 100
secured software distribution, 645
time-stamping, 644
management plane traffic, 376
management tools, 11
mandatory access control (MAC), 9, 246
  capability list, 247
  using a capability list approach, 247, 248
  using a matrix or lattice approach, 246
market-based regulations, 49
  principles based on requirements, 50
  standard require, 50
Maryland-based Lockheed, 24
MasterCard, 25, 49
M.3016 documents address, 641
media-handling functions, 383
media plane traffic, 376
media storage requirements, 13
memory management, 14, 412, 413
  base/bounds registers, 414, 415
  combining segmentation and paging (virtual memory), 419, 420
  fence, 413
  paging, 418–420
  relocation, 413, 414
  segmentation, 416–418, 420
memory management unit (MMU), 414
message authentication code (MAC), 83, 85
Message Digest algorithm version 5 (MD5), 82
MetroPCS, 295
metropolitan area networks (MAN), 274, 277–279
military link encryption devices, 522
MIP signaling messages, 354
MIPv4 application session packet tunneled rerouting, 356
MIPv4 functional components, 353
MIPv4 route modification signaling messages, 355
mission-critical, 38
mobile access, 385
mobile ad hoc networks (MANETs), 617
mobile IP (MIP) routing, 352
mobile notes (MNs), 354
mobile phones, 385
modern computer system security, 15
  twenty-first century tale, 15–17
  causes of occurence, 17–19
  prevention, 19–20

M
MAC, see mandatory access control (MAC)
MAC-based system, 9
Machine-readable rules, 647
Mac OS X malware, 512
MAC security, 528
mainframe computers, 1
malicious insiders, 52
malicious software (Malware), 503–505
management application protocols
  security, 368, 369
management functional group (FG), 381
management information bases (MIBs), 549, 635
management, involvement of, 170
management, of security mechanisms, 642–643
EMS security, 643
NMS security additions, 644
selected OSS/EMS security services, 644
  audit and logging, 645
  confidentiality and integrity, 645
  intrusion detection, 645
  key management, 644
  malicious software detection, 645
  nonrepudiation, 644
privilege and policy management, 644
<table>
<thead>
<tr>
<th>Index Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitoring, 13</td>
</tr>
<tr>
<td>activities, 14</td>
</tr>
<tr>
<td>tools, 13</td>
</tr>
<tr>
<td>Motorola 68000 family of processors, 411</td>
</tr>
<tr>
<td>Mozilla Firefox web browser, 423</td>
</tr>
<tr>
<td>MPLS signaling protocols, 351</td>
</tr>
<tr>
<td>label distribution protocol, 351</td>
</tr>
<tr>
<td>constraint-based, 351</td>
</tr>
<tr>
<td>resource reservation protocol, 352</td>
</tr>
<tr>
<td>RSVP traffic engineering, 352</td>
</tr>
<tr>
<td>MS Windows Internet Information Server (IIS), 19</td>
</tr>
<tr>
<td>MS Word documents, 35</td>
</tr>
<tr>
<td>Multi-blade equipment chassis, 650</td>
</tr>
<tr>
<td>multifactor authentication, 155</td>
</tr>
<tr>
<td>multi-level security (MLS), 254</td>
</tr>
<tr>
<td>multiprotocol label switching, 301–304</td>
</tr>
</tbody>
</table>

**N**

NAT. *see* network address translation (NAT)

National critical infrastructure, 56–59

National Incident Management System (NIMS), 656

National Infrastructure Protection Plan (NIPP), 58

cooperation with, 59

sector-specific plans, 58–59

National Institute of Standards and Technology (NIST), 657, 681

National Institutes of Science and Technology (NIST), 198, 260

available checklist categories, 198

developing a series of frequently asked questions (FAQs)

roles & responsibilities, and quick start guide documents, 199

Nessus, 667

.NET application framework, 636

evidence-based security, 622

microsoft designing, 622

role-based security, 622

security policy administration in, 623–624

web application security, 622

Netcat, 669

network access security model, 519

network address translation (NAT), 322, 536

operation, 324

network attachment control functions (NACFs), 384

network-based intrusion detection, 648

networked devices, 4

networked meetings, 51

networked systems, 24

network element layer (NEL), 397

networking architectures, 269

Internet network model, 272–274

major US telephone company, 269

OSI network model, 270–272

proprietary architectures for communications, 270

networking resources, 4

network management, converged, 393

network management layer (NML) systems, 396, 397

network management systems (NMS), 636, 644

network–network interface (NNI), 374

network operations centers (NOCs), 639, 646

Network Performance, Reliability, and Quality of Service Committee (PRQC), 262

network protocols, 295

layer 1—physical, 296

layer 2—data link protocols, 296, 297

data link layer complexity, 298

eternet, 297, 298

multi-drop interconnection, 297

point-to-point interconnection, 297

virtual ethernets, 299

layer 3—internetworking layer protocols, 310

layer 4—transport, 332

layer 5

management application protocols, 363

signaling and control application protocols, 349

user application protocols, 342

network security mechanisms, 4

network security technology, 4

network security toolkit (NST), 668

networks types, 274

network time protocol (NTP), 359

next-generation management, 650

next-generation operations systems and software (NGOSS)

business process framework, 397

NGN architecture, 372, 380, 381

NGN core and access networks, 372

NGN functional reference model, 380

strata, 380
NGN network level, major components, 375
core/services network domains, 376
customer network domain, 375
SP access network domains, 376
NGN transport and service domains,
relationship between, 389, 390
NGOs, 673
NIPP. See National Infrastructure Protection
Plan (NIPP)
NIST 800-37, 659
NIST guidelines, 662
NIST guide to protecting the confidentiality of
personally identifiable
information, 48
define PII, 48
NISTIR 7359, 659
NIST Special Publication 800-37, 199
NIST Special Publication 800-53, 199
Nmap, 668
non-IMS-compatible VoIP systems, 385
nonrepudiation, securing management, 644
Northrop Grumman Corp., 24
Northwest Bancshares Inc., 24
NSA (National Security Agency) hacker
team, 24
demonstration, how to break into, 24
supervisory-level access to networks, 24
NSA Information Assurance Technical
Framework (IATF), 199

O
OASIS. see organization for the advancement
of structured information standards
(OASIS)
objectives, 10, 61
object management group (OMG), 259,
264
object request broker (ORB), 626
objects, 63, 64
ongoing employee checks, 13
online retailers, 25
open Berkeley software distribution
(OpenBSD of unix), 462
open shortest path first (OSPF), 340
header field descriptions, 340
header structure and fields, 341
open systems interconnection (OSI)
model, 270
architecture, 271
contributions, formalization of concepts
for, 271
and Internet model layers, 272
layers, 270, 271
lower and upper layers, 270
open web application security project
(OWASP), 671
operating software, 409
types, 409
operating system (OS), 14, 245, 636
structure, 435–437
networking subsystem function, 437
security management function, 437
operational capabilities, 35
operational compliance, to regulations, 13
operational continuity, 55
operational costs, 36
operational security, 648
acceptance testing, 653
accountability, 653
accreditation and certification, 658
capability maturity model, 660
common criteria, 659
ISO 9000, 660
ISO 9001, 660
ISO 27001/27002, 660
compliance cycle major phases, 664
documentation, 653
field testing, 653
human resources and legal aspects, 653
independent auditing and review, 651–653
life-cycle review, 661
mechanism, 649
operational guidelines and
procedures, 650–651
operational readiness, 653
operational reviews, 657
operations compliance, 664
Center for Internet Security
(CIS)–Benchmark Tools, 666
compliance frameworks, 665
compliance verification process,
phases, 665
example security tools, 667–669
legislation/regulations, compliance
verification, 664
penetration testing, 669–671
penetration testing methodologies, 670
security compliance inventory, 666
security compliance procedures, 665
security compliance report, monitor, and improvement, 667
security compliance tools and checklists, 666
security event response and forensics, 655–657
senior security management mechanisms, 657
separation of duties and roles, 649–650
third-party access, 655
US department of defense 5220.22-M clearing and sanitization matrix, 663
withdrawal from service, 661, 662
operational security compliance program regular monitoring, 667
operational security compliance tools, 666
operations, administration, maintenance, and provisioning (OAM404, 646
operations compliance, 664
Center for Internet Security (CIS)—Benchmark Tools, 666
compliance frameworks, 665
compliance verification process, phases, 665
type example security tools, 667–669
legislation/regulations, compliance verification, 664
penetration testing, 669–671
penetration testing methodologies, 670
security compliance inventory, 666
security compliance procedures, 665
security compliance report, monitor, and improvement, 667
security compliance tools and checklists, 666
operations security controls, 13
corrective, 13
detective, 13
preventative, 13
recovery, 13
operations support systems (OSSs), 636, 638
billing, 639
engineering, 640
faultmanagement services, 639
outside plantmanagement, 640
testing services, 638–639
trouble ticketing systems, 640
operator, 473
order entry, securing management, 637
organization activities, 4
additional topic specific policy documents, 188
facilities, 3
sanctioned activities, 4
security policy, 3, 169
organization environments, 46
competition, 51–52
customer demands and expectations, 51
economic, legal, and political contexts, 47
legal liability, 51
market-based regulations, 49–51
regulations/legislation, 47–49
technology evolution, 51
terrorism and cybercrime, 52
organization for the advancement of structured information standards (OASIS), 163, 264, 591, 594
organization threat profile(s), 204
threat agents, 204, 214
attributes, 216
insider/outsiders, 214
origin integrity, 65
OS. see operating system (OS)
OSI model, 14
OS Login authentication, 242
OS Login function (process), 243
OS Login identifiers, 242
OS Login passwords, 243, 678
OSPFv2 authentication types, 341, 342
cryptographic, 342
null, 341
simple password, 341
OSSs. see operations support systems (OSSs)
outside plant management, 640
P
Packet Technologies and Systems Committee (PTSC), 262
pairwise transient key (PTK), 529
Parlay Group (Parlay), 265
passive optical networking (PON), 306, 382
access network, 307
terminals, 306
passive optical networks, protocol layering over, 308
passphrase, 158
password, 21, 23, 78, 108, 154, 158, 161, 203, 212, 243, 344, 462, 581, 678
password authentication protocol (PAP), 145
payment card industry (PCI) Council, 49
peering, 382
peer-to-peer (P2P) applications, 615–616
penetration testing, 669, 673
methodologies, 670
performance capabilities, 35
performance management activities, 634
permissions, 9
personal computers, 1
personal digital assistants, 385
personal identification numbers (PINs), 155
personally identifiable information (PII), 48
defined in European Union (EU) directive 95/46/EC, 48
State legislation regarding, 48
personnel security, 11
processes, 3
personnel training, 13
phishing, 21
physical and technical controls, 13
physical damage, 11
physical implementation, 373
physical security, 13
capabilities, 2
controls for, 13
ping flood, 327
ping of death, 327
PKCS. see public-key cryptography standards (PKCS)
PKIs. see public-key infrastructures (PKIs)
plain old telephone service (POTS), 306
plan approval, and implementation, 10
“plan, do, check, and act” (PDCA) concept model, 186
point of presence (POP) peering switches, 283
point-to-point protocol (PPP) servers, 145
policy hierarchy, 186
policy management, securing management, 644
port numbers (PAT), 322
post-employment procedures, 13
potential desirability, 372
power, 13
generation/distribution, 23
pre-employment screening, 13
pretty good privacy (PGP), 583–586
prevention, 6
primary administrator, 473
primary security-related hardware components, within a computer, 411
hardware encryption, 421
hardware acceleration cards, 422
hardware acceleration USB devices, 422
hardware security modules, 421, 422
Smartcards, 423, 424
interruption of processor activity, 420, 421
memory management, 412, 413
base/bounds registers, 414, 415
combining segmentation and paging (virtual memory), 419, 420
fence, 413
paging, 418–420
relocation, 413, 414
segmentation, 416–418, 420
processor states and status, 411
protection on the Intel 80386/80486, 412
protection on the Motorola 68000, 411, 412
printer managers, 9
priorities, 27
privacy, 1, 61
private data, 11
privileged authority, 221
privilege, securing management, 644
processing capacity, 2
product acquisition activity flow, 677
product certification, 658
professional hackers Linux assault kit (PHLAK), 668
program, 63
virus, 63
project/program management, 36
protections, 1, 26
mechanisms, 13
protocol layering over SONET, 311
protocol layers, 376, 377
provisioning, securing management, 638
proxy server, 599
PSTN Interconnection technologies, 281, 282
public-key cryptography standards (PKCS), 260
specifications, status, and usage, 261
public-key infrastructures (PKIs), 123, 128
certificate authority hierarchies, 131–136
certificate generation requests, 136–139
certificate verification, 143, 144
component deployment, 139–141
digital certificate revocation and status verification, 141, 142
X.509 digital certificates, 128–130
fields, 129, 130
public switched telephone network (PSTN), 279, 280, 294

Q
quality of service (QoS)
control mechanisms, 382
mechanisms/technology, 384
-related transport resource control, 384
quantitative risk analysis, 231
steps, 231

R
radio frequency (RF) “jamming,” 523
radio frequency (RF) patterns, 522
RADIUS protocol, 295
RADIUS server, 524
read-only memory (ROM), 157
real-time OS (RTOS), 409, 410
real-time transport protocol (RTP), 596, 597, 599
recovery, 7
Reed–Solomon coding, 99
re-evaluation, 38
reference validation mechanism (RVM), 429
registry, 482
data values, 484
hives, 483
key common data types, 484
root key permissions, 485
section descriptions, 483
regulations, 11, 25
regulations/legislation
deal with the protection of computer-related information, 47–48
information security driving, 49
reliability, 10, 26, 37–39, 63, 65, 262, 288, 601
reliable operation, 2
remote access, 654
remote authentication dial-in user service (RADIUS), 144
client and server, 145
remote network monitoring (RMON), 368
request for information (RFI), 673, 678
request for quote (RFQ), 673, 679
requests for information (RFI), 673, 678
requests for proposals (RFPs), 673, 676, 678
generally available (GA) date, 678
sample partial spreadsheet for inclusion, 680
requirements creep, 35
resolution, 38
resource and admission control functions (RACFs) act, 384
resource protection activities, 13
RFC identified authentication approaches, for MIPv4, 357
risk IT framework document, define domains, 189
risk evaluation, 190
risk governance, 189
risk response, 190, 191
risk IT practitioner guide, 191
comprise sections, 191
risk management framework, 224, 232
human originated threats, 239
impact analysis, 233, 234
non-human originated threats, 238
5-point impact scale, 239
5-point probability scale, 239
probability vs. impact composite values, 240
risk acceptance decision maker, 241
risk actionable, 241
risk assessment analysis, 234–236
risk assessment—asset definition and inventorying, 236, 237
risk assessment—threats, 237, 238
risk mitigation, 27, 224
approaches, ITU-T view, 224
common criteria (CC) mitigation approach, 227
ISO 27005 approach, to managing risk, 226
STRIDE mitigation approach, 226
role-based access control (RBAC), 249, 473
configuration files, 473
data types, 250
elements, 476
model, 473
procedures, 250, 251
roles, 249, 251
rootkits, 507, 509
type, 510
RSA decryption algorithm, 83, 86
RTP media protocols, 597

S
sandbox security model, 618
Sans Policy Project, 664
sashimi model, 32
schedules, 36
scope and plan initiation, 10
scrutinizing, 13
secret data, 25
secret military information, 1
secret service agent, 25
secured software distribution, 645
secure electronic transactions (SET), 150–154
  basic component of, 151
  capabilities provided by, 150
  dual signature, 151
  processes, 152
  subjects involved in SET transactions, 150
  transaction approach ensures, 153
Secure Hash Algorithm version 1 (SHA-1), 82
secure information systems, 2
secure/multipurpose internet mail extensions (S/MIME), 586–587
secure sockets layer (SSL), 574–581
secure time-stamping, 644
SecurID users, 24
securing management applications, 633
  FCAPS areas, 634
  management roots, 633–634
Securities and Exchange Commission (SEC), 260
security, 2, 13, 15
  account manager, 477
  branches of, 2
  RSA algorithm, 94
security administration, and configuration management, 223
vulnerabilities, 209, 210
security administrator tool for analyzing networks (SATAN), 668
security allocation, within NGN transport stratum, 393
security architecture, and models, 14
security assertion markup language (SAML), 594
  protocol, 594
  SAML 1.1, 595
  SAML 2.0, 595
  profile, 595
security mechanisms, 595
  single sign-on (SSO) use case, 596
security association database (SAD), 541, 549
security audit, 220
  log vulnerabilities, 207
security awareness, 11
security breach at EMC Corp.’s RSA, 24
security certification, definition of, 658
security checklist for web applications architecture MSDN, 666
security compliance inventory, 666
security compliance procedures, 665
security compliance report, 667
security compliance tools and checklists, 666
security configuration management, 647
security context, 431
security controls, 13
security credentials, 25
security-critical functions, 428
security design for protocol layer 1, 520
  wired and optical media, 520
  dial-back modems, 522
  link-bulk encryption, 520, 522
  wireless media, 522, 523
  fast frequency hopping, 523
security design, for protocol layer 3, 530
  alarm settings, 552
basic NAT operation, 553
combining security associations, 542–543
device IPSec setting values, 551
documents on NAT, 554
ESP transforms, 545
IKE operation, 537
  general IKE settings, 550
  IKE message settings, 538
negotiation messages, 540
sequence of message exchanges and activities, 538–539
versions of IKE, 540–541
IKE v1 major RFCs, 558
IKE v2 major RFCs, 558
IP security (IPsec), 530–531
AH header field usage, 544
architecture, 531–536
authentication header (AH)
transform, 544
AH header field usage, 544
AH header structure, 544
components location in, 532
encapsulating security payload (ESP)
transform, 545
ESP transforms, 546
and fault-tolerant network designs, 554–556
general settings, 550
IKE AH ignored header bits, 535
implementation availability, 554
and IP MIBs, 549
IP packet within IP packet tunneling, 534
key management and key exchange, 536, 537
modes and transforms compared, 537
and network address translation, 549, 551
packet receipt processing, 548
packet transmission processing, 547
and PKI, 556–557
policy management, 547
processing, 545
pull technique, devices, 549
secure remote access and secure VPN examples, 533
security associations (SAs), 541–542
summary and observations, 557
transport and tunnel modes, AH and ESP header placement, 536
NAT ingress problem, 552
NAT traversal and IPSec, 553
packet header placement for ESP SAs within ESP SAs, 546
subject identity field settings on the device, 550
security domain, 64, 65
bi-lateral agreements, 65
security rules, 65
security event manager (SEM), 668
security frameworks (X.810–X.816), 402
security goals, 61
objectives, 65
security governance, 169, 199
security identification number (SID), 478, 482
security elements, 482
security identifiers (SIDs), 478, 481
security in application signaling, and control protocols, 364, 365
security incident management, 655
security management
activities, 634
focuses, 169
functional entities, 647
goals and objectives, 170, 171
practices and guidelines, international standards, 171
and standards, 170
system, 646
security management framework, 645
functional entities, 647
administrative account management, 648
authentication credentials management, 648
security configuration management, 647
security event, fault, and attack management, 647
verification and validation management, 648
functions defined in M.3410, 646
organizations, 646
security measures, 14
security mechanisms, 2, 77, 80
management of, 633
specific examples, 80–81
security mechanisms, for deployed operating systems (OSs), 437
desirable GP OS platform hardware security-related mechanisms, 439
general purpose (GP) OSs, 438
GP OS context security-related software functions, 443–448
hardware mechanisms descriptions, 440–442
for GP OS usage, 438
for minimized GP OS usage, 449
security mechanisms, for deployed operating systems (OSs) (Continued) minimized general purpose operating systems, 438, 449 software functional entities, 438 software mechanisms for minimized GP OS usage, 449 security operations centers (SOCs), 646, 656 security policy decision function (SPDF), 429 security policy enforcement function (SPEF), 429 security reference monitor (SRM), 477 security-related extensions, 332 security-related standards, 251 security services, 61, 403 alternative, applicability of, 77 applicability of alternative services, 77 mapping of, 75, 76 and security mechanisms, comparison, 78–79 security services, modern definition, 69 accountability, 73 logging and auditing, 73 non-repudiation with proof of delivery, 73 non-repudiation with proof of origin, 73 authentication services, 69 data-origin authentication, 69 peer-entity authentication, 69 user authentication, 69 authorization-access control, 69, 70 availability, 71 human-caused disasters, 71 human-caused malicious actions, 71 natural disasters, 71 prevention of service access denial, 72 prevention of service failure, 72 restoration/continuity of services and information, 72–73 service platform functionality, 72 integrity, 70 data integrity, 71 information integrity, 70 separation of duty, 70 well-formed transactions, 71 privacy as a security service, 74 service mapping and application of services, 74 security standards, 259, 260 security tokens, 24 security vulnerabilities, 213 SekChek local, 668 senior management oversight, 170 sensor networks, 288, 289 separation of duties, 649 service charities, 53 service control functions (SCFs), 384 service management layer (SML) management systems, 396, 397 service-oriented architecture (SOA), 590 WS-security policy for, 593 service providers (SPs), 52, 62, 279, 371, 636 access and backbone metropolitan optical networks, 382 access domain, 374 core/services domain, 374 Data Link layer, 377, 378 internal NNI (INNI), 376–380 internetworking, 377–379 protection (see service providers (SPs), protection) SP MAN access network(s), 372 two end nodes and one SP, 378 service providers (SPs), protection access to only authorized features, 62 compliance, 62 confidentiality, 62 error-free and non-malicious interaction, 62 integrity, 62 service stratum, 385 and IP Multimedia Subsystem (IMS), 385 NGN functions in, 384 Session Boarder Control (SBC) function, 598, 605 functionality, within AER, 604 session description protocol (SDP), 597 SET. see secure electronic transactions (SET) shared libraries, 673 short-term plan, 10 signaling, and control application protocols security, 363 signaling and control plane traffic, 376 signal transfer points (STPs), 283 signature algorithms, 607 Siloed management system structuring, 398 SIMILAR systems engineering process, 32, 34 assess performance, 38
develop/integrate, 36, 37
investigate alternatives and model the system, 35, 36
launch the system, 37, 38
re-evaluation, 38
stating the problem, 34, 35
simple network management protocol (SNMP), 363, 634
security issues, 367
SNMP version 1 (SNMPv1), 366
SNMP version 2 (SNMPv2), 366
SNMP version 3 (SNMPv3), 366
simple network time protocol (SNTP), 359
simple object access protocol (SOAP), 593
specification, 593
single sign-on (SSO) system, 159–163
identity management (IdM), 164–167
categories, 167
Shibboleth SSO authentication, 164
SIP call processing/signaling message flow, 600
SIP responses, 599
SIP signaling and media security, 601
SIP signaling protocol, 597
smartcards, 155, 158, 423, 424
smart phone, 294
Smurf attack, 327
SNMP, see simple network management protocol (SNMP)
software, 4
-based system, 636
detection, 645
licensing, 12
malicious, 25
piracy, 12
security, 9
Software Engineering Institute (SEI), 41
software protects information, 424
definitions of OS terms, 425
operating system, offer protection, 426
isolation, 426
share all or share nothing, 426
share by capabilities, 426
share via access limitation, 426
software layering, by protection ring, 425
Solaris operating system, 462, 473
elements, 473
Sonet optical rings, 309
Sonet STM-1 structure, 310
specifications, 39
specific operating systems, 461
SP 800-27 “Engineering Principles for Information Technology Security (A Baseline for Achieving Security”), 199
Sprint Nextel, 295
SPs, see service providers (SPs)
spyware, 21, 510, 511
SQL injection attack, 9
SS7 protocols, 283
standard generalized markup language (SGML), 589
Standards Development Organizations (SDOs), 259, 260
state management, 14
statement of work (SOW), 679
static libraries, 673
steal intellectual property, 11
storage media, 13
stream control transmission protocol (SCTP), 334, 339
header, 339
stream encryption algorithm, 88
usage, 88
stream symmetric encryption algorithms, 90
subjects, 63, 64
sub-net mask, 323
(sub-)system components, 36
supervisory control and data acquisition (SCADA) systems, 284, 286–288
symmetric encryption algorithms, 11, 83, 88
Advanced Encryption Algorithm (AES), 88
CBC encryption and decryption, 91
propagating, 91
cipher-block (CB) or electronic code book (ECB) mode, 90
cipher feedback (CFB) encryption and decryption, 92
counter (CTR), 92
Digital Encryption Standard (DES), 88
International Data Encryption Algorithm (IDEA), 88
operate on blocks of plain-text, 90
operational modes, 90
output feedback (OFB), 92
triple digital encryption standard (3DES or TDES), 88
symmetric encryption algorithms (Continued) use of a secret key, 92
Diffie–Hellman key exchange algorithm, 92
key distribution centers (KDCs), 92
static or dynamic approaches, 92
symmetric encryption based MAC data integrity, 85
synchronous transport module (STM-1), 309
system access control list (SACL), 478, 479
system administrator, 473
system administrator’s integrated network tool (SAINT), 668
system controls, identification, authentication vulnerabilities, 205, 206
system integrity, 221
and privileged authority vulnerabilities, 208
Systems and Software Consortium (SSCI), 46
systems engineering, 31, 32
“define system architecture” phase, 39, 40
sub-activities within, 40
defining customer needs and, 32
documentation spanning, 40
engineering process, for complex systems, 39
ISO 9000 processes and procedures, 41–43
major activities, 33
process management, 41
process variations, 41
products, 37
systems engineering capability model (SECM), 46
systems implementation or procurement, 671–672
acceptance testing and review, 681
CMMI and ISO-9001 processes, 672
coding, 672, 673
development, 672
OS Login Passwords, 678
procurement, 673
product acquisition activity flow, 677
request for quote (RFQ), 679
requests for information/proposals (RFIs/RFPs), 673, 676
sample partial spreadsheet for inclusion in an RFP, 680
standards compliance, 679
statement of work (SOW), 679
testing, 673
system software problems, 14
system validation, 32
T
TCP, see transmission control protocol (TCP)
TCP/IP (Transmission Control Protocol/Internet Protocol), 272
technical complexity, 36
technical controls, 13
Telecom Management and Operations Committee (TMOC), 262
telecommunications management network (TMN), 634, 635
abstract architecture, 396
ANSI Standard ATIS-0300074, 646
element/network management systems/operations systems, 636–640
layers and functional areas, 396
management networking security, 640
organizational layers, 635
security, 640–642
service management, 642–643, 645
structure, 635–636
telecommunications service providers (TSPs), 279, 637
TeleManagement Forum (TMF), 259, 265, 397
temporal key integrity protocol (TKIP), 529
tenets of security, 11
testing services, securing management, 638
text-voice-video integrated web browsing, 51
third-Generation Partnership Project (3GPP), 260, 262, 295
threat agent (attacker), 224, 518
targets, 219
and objectives, 217
threats, 11, 22, 203, 224, 641
analysis
ITU-T X.800 approach to, 225
ITU-T X.805 approach to, 226
category, 641
denial-of-service attacks, 22
mapping STRIDE threat categories to, 226
poor passwords, 22
poor security practices, 23
program flaws, 22
social engineering, 22
Spyware, 22
Trojan horses, 22
viruses, 22
and vulnerability analysis, 201
worms, 22
“Tier 2” policies with organizations, 188
“Tier 1” policy documents, 187
time division multiplexed (TDM) interfaces, 306
TLS. see transport layer security (TLS)
TMF. see TeleManagement Forum (TMF)
TMN. see telecommunications management network (TMN)
tools, 26
trade-off analyses, 31
traffic classification, 382
training, 11
transmission control protocol (TCP), 332, 334
frequently encountered and UDP port numbers, 336, 337
header, 335
three-way handshake, 335
vulnerabilities in, 338
transmission methods, 14
transportation, 23
transport control functions, 384
transport formats, 14
transport functionality, 381
transport layer protocols security, 342
transport layer security (TLS), 574–581
protocol, 342
and security capabilities, 343
transport protocol feature comparison, 334
transport security protocols, 573–582
datagram transport layer security (DTLS), 574–581
in Internet protocol stack, 574
secure shell protocol (SSH), 581
secure sockets layer (SSL), 574–581
SSL/TLS/DTLS/IPsec, comparison of, 581–582
TLS/SSL/DTLS, within protocol stack, 574–576
SSL virtual private networks, 579–581
TLS operational activities, 579
TLS session establishment, 576–579
TLS/SSL security items, 579
transport stratum, 381
TRAP instructions, 411
Trojan horse, 507–509
payloads, types, 508
trouble management, 38
trouble ticket, 638, 639
trouble ticketing systems, 640
trust, 61, 63, 64
trusted computer security evaluation criteria (TCSEC), 14
TSPs. see telecommunications service providers (TSPs)
TSP vs. customer premise equipment, 284
T1 trunk and ISDN digital 1 (DS1) trunk framing, 283
turbo coding, 100
turf conflicts, 650
“turnkey” system, 36
twinge attack, 327
U
UDP. see unreliable datagram protocol (UDP)
unacceptable behavior, 3
unauthorized disclosure, 11
uniform resource identifier (URI), 598
universal subscriber identity module (USIM), 294
unix and linux security, 462
access control, 464–467
audit logs, 467
group accounts, 463
inetd and TCP wrappers, 469
inetd.conf file contents, 469
intrusion detection, 467
log files, 470
Login and User Accounts, 462, 463
programs that produce log events, 468
set group ID (setgid), 463, 464
set user ID (setuid), 463, 464
syslog.conf example contents, 469
system log, 468
TCP wrapper arguments, 470
typical log files, 467
unix disk partitions, 470
unix/linux file system, typical main components of, 471, 472
unix/linux file system proposed components partitioning for, 474
unix malware, 512
UNIX operating systems, 249
Unix ‘rm’ command, 662
unreliable datagram protocol (UDP), 334, 338
common application protocols using, 339
header, 338
US Department of Defense (DoD), 260
Advanced Research Projects Agency (ARPA), 295
5220.22-M
sanitization matrix, 663
User Agent (UA) software, 18
user application protocols security, 349
user datagram protocol (UDP), 335
user friendly, 2
user–network interface (UNI), 374
user plane traffic, 376
user service application protocols
e-mail, 583
pretty good privacy (PGP), 583–586
secure/multipurpose internet mail
extensions (S/MIME), 586–587
S/MIME/OpenPGP differences, 587

V
vendor-supplied components, 38
ventilation, 13
verification, 31
methodologies, 37
operational functionality and performance
capabilities, 37
operational processes and procedures, 37
requirements compliance of supplier
components, 37
verification tests, 654
Verizon Wireless, 295
virtual ethernets (VLANs), 299
canonical format indicator, 299
priority code point (PCP), 299
802.1q Ethernet frame, 299
Tag Control Information (TCI), 299
Tag Protocol ID (TPID), 299
VLAN IDenti fier (VID), 300
virtual routers, 649
viruses, 505, 615
types, 506–507
Visa, 25, 49
VLANs. see virtual ethernets (VLANs)
voice over internet protocol (VoIP), 307, 351, 596
applications, approaches for attacking, 599
device security, 602
H.323 signaling protocols and RTP media
protocols, 597
Internet phone service, 17
media security, 601
and NAT, 604
session border control, 602
signaling security, 599
VoIP SP MAN infrastructure, 603
voice–video conferencing, 51
VoIP. see voice over internet protocol (VoIP)
vulnerabilities, 12, 203, 224
application-specific, 203
asset, 204
categories, 203
configuration, 203
operating system, 203
protocol-specific, 203
W
war dialing, 522
waterfall model, 32
wavelength division multiplexing
(WDM), 308
web browser, 589, 594
single sign-on (SSO), 595
web pages, 376
web services, 593
web services description language
(WSDL), 593
websites
faked ecommerce, 21
shut down, 25
Wells Fargo & Co., 24
white box, 665
wide area networks (WAN), 274, 278, 279
WiFi, 274, 277, 297, 370
WiMAX Forum, 295
WiMAX technology, 295, 385
Windows live passports, 423
Windows operating systems, 22, 476, 477
default groups and user rights assigned
to, 477
users and groups, 477
Windows security architecture, 477
Windows Server 2003 operating system,
492
authentication protocols, 492, 493
identification, 493
LSA architecture, 494
role-based access control (RBAC), 493–496
model, 496
SSPI architecture, 495
wireless access, 385
wireless LAN (WLAN), 274, 277, 385
wireless mesh network (WMN), 617
wireless networking, 300, 301
customer edge router (CER), 301
ISM bands of radio frequencies, 300
802.11 set of wireless LAN (WLAN) standards, 301
war-driving, 301
weaknesses in WEP-based LAN security design, 301
wireless sensor network (WSN), 289, 617
wireless technologies, 382
Wireless Technologies and Systems Committee (WTSC), 262
Wireshark, 668
WorldCom, 46
World Wide Web (Web), 589
World Wide Web Consortium (W3C), 259, 265
worms, 507, 615
WS-Security, 593

X
XML-based languages, 265, 636
XML encryption, 592
XML signatures, 591
XML web services, 637
X.800 Security services, 66–67
access control, 67
authentication, 67
data-origin, 67
peer-entity, 67
user, 67
confidentiality, 67
connection, 68
connectionless, 68
selective field, 68
traffic flow, 68
data integrity, 68
connection integrity without recovery, 68
connection integrity with recovery, 68
connectionless integrity, 68
selective field connection integrity, 68
selective field connectionless integrity, 69
non-repudiation, 69
non-repudiation with proof of delivery, 69
non-repudiation with proof of origin, 69
X Window system, 346

Y
Yersinia, 668