

Index

Note to the Reader: Throughout this index page numbers in bold indicate primary discussions or definitions of a topic. Italicized page numbers indicate illustrations.

Numbers

8.3 naming conventions, **63**
 10Base2/Thinnet cable, **83**
 10Base5/Thicknet cable, **83**
 10BaseT cable, **85, 86**
 100BaseT cable, **86**
 802.11/11x wireless networks, **40,**
 40–41, 65
 1000BaseT cable, **86**

A

AAA servers, **43**
 acceptable use policy, **163**
 acceptance of risk, **172**
 access control, *See also* remote access
 in cryptography, **128**
 in physical security, *See also*
 operational
 barriers, **151–152, 152**
 biometrics, **14–15, 152**
 defined, **150–151, 151**
 mantraps, **152, 152**
 security guards, **152**
 to resources, *See also* Security+
 defined, **3**
 Discretionary Access Control, **5–6**
 exam essentials on, **6–7**
 Mandatory Access Control, **4–5**
 overview, **3–4, 168, 169**
 Role-Based Access Control, **6**
 access hooks, **21**
 account lockout, **164**
 ACLs (access control lists), **5, 107**
 active detection and response, **98,**
 99–100
 ActiveX vulnerability, **57**
 ad hoc mode, **66**
 agents, **18**
 AH (Authentication Header)
 protocol, **45**
 ALE (Annual Loss Expectancy)
 formula, **172**
 alternate sites, **157–158**
 amplification networks, **19**
 anomaly detection, **97, 98**
 anonymous FTP, **62–63**
 application hardening. *See* environment
 application-level gateway firewalls, **76**
 architecture documentation, **175**
 ARO (Annualized Rate of Occurrence)
 formula, **172**
 asset identification, **172**
 asset inventories, **176**
 assignment of risk, **172**
 asymmetric encryption, **49–51, 50–51,**
 123, 126, 127
 attack methods, *See also* IDSs;
 Security+; vulnerabilities
 back door, **21–22, 22**
 birthday, **26, 120**
 broadcast storm, **92**
 buffer overflow, **27, 57–58**
 Denial of Service attacks
 bonk and boink, **21**
 countermeasures against, **21**
 defined, **18**
 Distributed DOS, **19, 19**

182 attack surfaces – broadband signaling

- Distributed Reflective DOS, 19
 - fraggle, 19
 - land, 21
 - ping flood, 21
 - ping of death, 21
 - smurf, 19, 20
 - SYN flood, 20, 20
 - teardrop, 20, 20
 - eavesdropping, 56–57
 - exam essentials on, 28–29
 - on hashing, 120–121
 - malicious code
 - defined, 29
 - exam essentials on, 30
 - logic bombs, 30
 - Trojan horses, 30
 - viruses, 29
 - worms, 30
 - man-in-the-middle, 23, 23
 - mathematical, 25
 - overview, 18
 - packet sniffing, 56–57, 63, 78
 - password cracking, 12, 26–27, 120–121
 - replay, 24, 24
 - reverse hash matching, 26, 120
 - social engineering, 31–32, 52–53, 153
 - software exploitation, 27
 - spoofing, 22–23, 52
 - TCP/IP hijacking, 24, 25
 - war dialing, 79
 - attack surfaces, 15
 - attenuation, 83
 - auditing
 - audit trails/logs, 32, 33, 176
 - defined, 32–33
 - privileges, 169
 - using SNMP protocol, 81
 - authentication, *See also* Security+
 - in cryptography, 127
 - defined, 3
 - methods
 - biometrics, 14–15, 152
 - certificates, 10–11, 11
 - CHAP, 9–10, 10
 - defined, 7
 - exam essentials on, 15
 - Kerberos, 7–9, 9
 - multi-factor authentication, 13–14, 14
 - mutual authentication, 14
 - tokens, 13, 13
 - usernames/passwords, 12, 12
 - strong authentication, 14
 - tools
 - RADIUS, 42–43, 43
 - supported by L2TP/PPTP protocols, 44
 - TACACS, 43, 43
 - authentication servers, 110
 - authorization, 3, *See also* access control
 - availability, 160
-
- B**
- back door attacks, 21–22, 22
 - backups, 156–157, 161
 - bag and tag process, 171
 - baseband signaling, 85, 85
 - biometrics, 14–15, 152
 - birthday attacks, 26, 120
 - blind FTP, 63
 - block cipher cryptography, 122
 - BNC connectors, 83, 83–84
 - boink/bonk attacks, 21
 - boot sector viruses, 29
 - bots, 18
 - bounce networks, 19
 - bridge trusts, 132, 133
 - broadband signaling, 85, 85

brute-force attacks, 27
 buffer overflow attacks, 27, 57–58
 business continuity, *See also* operational
 backups, 161
 defined, 159
 elements in planning, 159–160
 exam essentials, 162
 high availability/fault tolerance,
 160–161
 utilities, 160

C

callback feature, 79
 CD-R disks, 88
 centralized key management, 136–137,
 137, 138, 139
 centralized privilege management, 168
 certificates, *See also* cryptography
 certificate authorities, 10, 129, 130
 certificate policies, 131
 certificate practice statements, 131
 defined, 10–11, 11, 129
 destruction, 141
 expiration, 139
 obtaining, 10–11, 11, 130–131
 renewal, 140–141
 revocation, 131–132, 132, 139
 status checking, 139, 140
 storage, 138
 suspension, 140
 trust models, 132–134, 133
 trusted third parties, 10, 129
 X.509 certificates, 129, 130
 certification credentials, 174
 CGI (Common Gateway Interface), 58
 chain of custody, 170
 change documentation, 176

CHAP (Challenge Handshake Authentica-
 tion Protocol), 9–10, 10
 circuit-level gateway firewalls, 76
 classification labeling, 4, 176
 clearance levels, 4–5
 clients, 81
 clustering servers, 160, 162
 coaxial cable, 83–85, 83
 code of ethics policy, 165–166
 cold sites, 157–158
 common routers, 76
 communication security, 39–70, *See also*
 Security+
 directory security, 60–61, 61
 e-mail security
 using digital signatures, 50–51, 51
 exam essentials on, 53–54
 using filters, 52
 hardening e-mail servers, 1
 08–109, 108
 hoax e-mail, 52–53
 MIME headers and, 51
 overview, 48, 49
 using PGP encryption, 50
 using S/MIME encryption,
 49–50, 50
 spam e-mail, 52
 spoofed e-mail, 52
 vulnerabilities, 51–53
 File Transfer Protocol
 anonymous FTP, 62–63
 blind FTP, 63
 defined, 62
 exam essentials on, 63–64
 file sharing, 63
 overview, 61–62
 Secure FTP, 62
 vulnerabilities, 63
 Internet security
 ActiveX and, 57

- buffer overflow attacks, 57–58
- cookies and, 58
- exam essentials on, 59–60
- HTTP protocol and, 54–55, 55, 56
- using HTTPS protocol, 56
- instant messaging and, 56–57
- JavaScript and, 57
- overview, 54–55, 55
- using S-HTTP protocol, 56
- signed applets and, 58
- SMTP relay and, 58–59
- using SSL encryption, 55–56
- using TLS encryption, 55, 56
- vulnerabilities, 56–59
- remote access security
 - in 802.11/11x wireless, 40–41, 40, 65
 - exam essentials on, 47–48
 - in IPSec protocols, 44–46, 45–46
 - in L2TP protocol, 44
 - overview, 39–40, 39
 - in PPTP protocol, 44
 - using RADIUS, 42–43, 43
 - using Secure Shell, 44
 - using TACACS, 43, 43
 - in virtual private networks, 41–42, 41
 - vulnerabilities, 46–47
- review question answers, 70
- review questions, 68–69
- wireless security
 - in 802.11/11x networks, 40–41, 40, 65
 - exam essentials on, 66–67
 - overview, 64
 - vulnerabilities, 66
 - using Wired Equivalent Privacy, 65
 - using WTLS in WAP protocol, 64–65, 65
- communication in security training, 174
- confidentiality, 4, 125, 125
- containment, 102, 166
- cookies, 58
- CPSs (certificate practice statements), 131
- CRLs (certificate revocation lists), 131–132, 132
- cross certification, 132, 133
- cryptography, 119–146, *See also* Security+
 - cryptographic algorithms
 - asymmetric encryption, 49–51, 50–51, 123, 126, 127
 - exam essentials, 124
 - hashing, 26, 119–121, 120
 - overview, 119
 - symmetric encryption, 46, 121–122, 126–127, 127
 - encryption protocols
 - for e-mail, 49–51, 50–51
 - IPSec, 44–46, 45–46
 - Pretty Good Privacy, 50–51, 51
 - for remote access, 44–46, 45–46
 - S/MIME, 49–50, 50
 - Secure Sockets Layer, 55–56
 - Transport Layer Security, 55, 56
 - for web browsers/servers, 55–56
 - key and certificate management
 - centralized key management, 136–137, 137, 138, 139
 - decentralized key management, 137–138, 137
 - destruction, 141
 - exam essentials, 141–143
 - expiration, 139
 - key disasters, 138
 - key management rules, 136
 - key usage, 141
 - M of N key control, 140
 - multiple key pairs, 141
 - overview, 136

private key escrow, 138–139, 139
 private key protection, 138
 recovery from escrow, 140
 renewal, 140–141
 revocation, 131–132, 132, 139
 status checking, 139, 140
 storage, 138
 suspension, 140

Public Key Infrastructure
 certificate authorities, 10, 129, 130
 certificate policies, 131
 certificate practice statements, 131
 certificate revocation,
 131–132, 132
 defined, 10–11, 11, 122, 129
 exam essentials, 134–135
 obtaining certificates, 10–11, 11,
 130–131
 trust models, 132–134, 133
 trusted third parties, 129
 X.509 certificates, 129, 130

review question answers, 146
 review questions, 144–145

security services
 access control, 128
 authentication, 127
 confidentiality, 125, 125
 digital signatures, 126–127,
 127, 128
 exam essentials, 128–129
 integrity, 125–127, 127
 nonrepudiation, 128
 overview, 125

standards and protocols, 135

vulnerabilities
 hashing, 26, 120–121
 key recovery, 140
 key storage, 137, 138
 weak keys, 25

D

DAC (Discretionary Access Control),
 5–6, 7, 164, 168, 169

data centers. *See* server rooms

data repository servers, 110

database servers, 111

DDOS (Distributed Denial of Service),
 19, 19, *See also* DOS

decentralized key management,
 137, 137–138

decentralized privilege management, 168

DHCP (Dynamic Host Configuration
 Protocol) servers, 110

diagnostics. *See* auditing

dictionary attacks, 27

differential backups, 157

digital signatures
 using asymmetric encryption, 50–51,
 51, 126
 defined, 126
 for nonrepudiation, 50, 128
 signed applets, 58
 using symmetric encryption,
 126–127, 127

directory security, 60–61, 61

directory services, 61, 61, 110, 111

disaster recovery, *See also* operational
 alternate sites, 157–158
 backups, 156–157
 exam essentials, 158–159
 offsite storage, 157
 overview, 156
 plans, 158
 secure recovery, 157

disclosure, 4

diskettes, 88

disposal/destruction policy, 165

186 DMZs (demilitarized zones) – environment hardening

- DMZs (demilitarized zones), 62, 76, 90, 90
- DNS (Domain Name Service) servers, 109
- documentation. *See* security documentation
- domain controllers, 110
- DOS (Denial of Service) attacks, *See also* attack
 - bonk and boink, 21
 - buffer overflows as, 57–58
 - countermeasures against, 21
 - defined, 18
 - Distributed DOS, 19, 19
 - Distributed Reflective DOS, 19–20, 20
 - on e-mail, 51
 - fraggle, 19
 - land, 21
 - ping flood, 21
 - ping of death, 21
 - smurf, 19, 20
 - SYN flood, 20, 20
 - teardrop, 20, 20
- dual-homed firewalls, 76, 77
- due care, 164
- DVD-R disks, 88

E

- 802.11/11x wireless networks, 40, 40–41, 65
- e-mail security, *See also* communication
 - using digital signatures, 50–51, 51
 - exam essentials on, 53–54
 - using filters, 52
 - hardening e-mail servers, 108–109, 108
- overview, 48, 49
- using PGP encryption, 50
- using S/MIME encryption, 49–50, 50
- vulnerabilities
 - corrupted MIME headers, 51
 - hoaxes, 52–53
 - open relays, 59
 - overview, 51
 - SMTP relays, 58–59
 - spam, 52
 - spoofed e-mail, 52
- education on security, 174
- EF (Exposure Factor) formula, 172
- EMI (electromagnetic interference), 85, 86, 154, 154
- employee termination policy, 165
- encapsulation, 42
- end-user computers, 81
- environment hardening, *See also* infrastructure
 - application hardening
 - data repository servers, 110
 - database servers, 111
 - defined, 16, 107
 - DHCP servers, 110
 - directory services, 110, 111
 - DNS servers, 109
 - e-mail servers, 108–109, 108
 - file servers, 109–110, 110
 - FTP servers, 109
 - NNTP servers, 109
 - print servers, 110
 - using updates, 107
 - web servers, 108
 - defined, 16
 - documenting, 103
 - exam essentials, 111–112
 - network hardening
 - using access control lists, 107

configuration issues, 106–107
defined, 106
enabling/disabling services, 107
using updates, 106
OS/NOS hardening
defined, 103–104
file systems, 104–105
using updates, 105
overview, 103
security baselines and, 103
escrow, key, 138–139, 139, 140
ESP (Encapsulating Security Payload)
protocol, 45
evidence. *See* forensics
extranets, 90, 91

F

false positives, 95
FAT (File Allocation Table), 105
fault tolerance, 160–161
fiber optic cable, 87, 87
file server hardening, 109–110, 110
file system hardening, 104–105
File Transfer Protocol. *See* FTP
filters, *See also* firewalls
defined, 74
e-mail filters, 52
ingress filters, 78
fire suppression, 154–155
firewalls, 74–77, 75, 77, 95, 96
firmware, 106
flashcards, 88
floppies, 88
forensics, *See also* operational
chain of custody, 170
collection of evidence, 171
defined, 170

evidence preservation, 170–171
exam essentials, 171
fraggle attacks, 19
FTP (File Transfer Protocol), *See also*
communication
anonymous FTP, 62–63
blind FTP, 63
defined, 62
exam essentials, 63–64
file sharing, 63
FTP servers, 109
overview, 61–62
Secure FTP, 62
vulnerabilities, 63
full backups, 156

G

guidelines, 175

H

hard drives, 88
hardening. *See* environment
hashing, *See also* cryptography
attacks on, 120–121
defined, 26, 119–120, 120
digital signatures and, 50–51, 51
hierarchical trusts, 132, 133
high availability, 160–161
hiring policy, 165
hoax e-mail, 52–53
honey pots, 100–101, 101
host-based IDSs, 97, 97
hot sites, 157, 158
hotfixes, 105
HR (human resources) policy, 165–166

188 HTML (Hypertext Markup Language) – infrastructure security

HTML (Hypertext Markup Language),
54–55, 55

HTTP (Hypertext Transfer Protocol),
54–55, 55, 56

HTTPS (HTTP over SSL) protocol, 56

I

IDSs (Intrusion Detection Systems),

See also infrastructure

active detection/response, 98, 99–100

anomaly detection, 97, 98

defined, 81, 95, 96

exam essentials, 102

false positives, 95

honey pots, 100–101, 101

host-based IDSs, 97, 97

incident response, 101–102

network-based IDSs, 96, 96

passive detection/response, 98

signature detection, 97, 98

IEEE 802.11/11x wireless networks,
40, 40–41, 65

IKE (Internet Key Exchange), 46

IM (instant messaging), 56–57

IMAP (Internet Message Access
Protocol), 48

incident response policy, 166

incremental backups, 157

infrastructure mode, 66

infrastructure security, 74–115,

See also Security+

environment hardening, *See also*

environment

application hardening, 107–111,

108, 110–111

documenting, 103

exam essentials, 111–112

network hardening, 106–107

OS/NOS hardening, 103–105

overview, 103

security baselines and, 103

using updates, 105, 106, 107

Intrusion Detection Systems

active detection/response,

98, 99–100

anomaly detection, 97, 98

containment, 102

defined, 81, 95, 96

exam essentials, 102

false positives, 95

honey pots, 100–101, 101

host-based IDSs, 97, 97

incident response, 101–102

network-based IDSs, 96, 96

passive detection/response, 98

signature detection, 97, 98

media security

CDs/DVDs, 88

coaxial cable, 83, 83–85

exam essentials, 88–89

fiber optic cable, 87, 87

flashcards, 88

floppies/diskettes, 88

hard drives, 88

overview, 82

removable media, 87–88

shielded cabling, 85–86, 85–86,

154, 154

smartcards, 88

tape drives, 87

unshielded cabling, 85–86, 85–86

review question answers, 115

review questions, 113–114

security devices, *See also* IDSs

exam essentials on, 82

firewalls, 74–77, 75, 77, 95, 96

Intrusion Detection Systems, 81,

95–102, 96–101

- mobile devices, 82
- modems, 79, 79
- for monitoring/diagnostics, 81
- Remote Access Server, 80
- routers, 77–78, 77–78
- servers, 81
- switches, 78, 78
- Telecom/PBX systems, 80, 80
- virtual private networks and, 81
- wireless security, 79
- workstations, 81
- security topologies
 - defined, 89
 - demilitarized zones, 90, 90
 - exam essentials on, 94–95
 - extranets, 90, 91
 - intranets, 90, 91
 - IP address translation and, 93–94, 93
 - RFC 1918 and, 93–94
 - security zones, 89–90, 89–91
 - tunneling and, 94
 - virtual LANs, 91–92, 92
- ingress filters, 78
- instant messaging (IM), 56–57
- integrity, data, 125–127, 127
- Internet Key Exchange (IKE), 46
- Internet Message Access Protocol (IMAP), 48
- Internet security, *See also*
 - communication
 - exam essentials on, 59–60
 - using HTTPS protocol, 56
 - overview, 54–55, 55
 - using S-HTTP protocol, 56
 - using SSL encryption, 55–56
 - using TLS encryption, 55, 56
 - vulnerabilities
 - ActiveX, 57
 - buffer overflows, 57–58

- Common Gateway Interface, 58
- cookies, 58
- HTTP protocol, 54–55, 55, 56
- instant messaging, 56–57
- JavaScript, 57
 - signed applets, 58
 - SMTP relay, 58–59
- intranets, 90, 91
- IP address translation, 93, 93–94
- IPSec (Internet Protocol Security)
 - protocols, 44–46, 45–46
- ISAKMP (Internet Security Association and Key Management Protocol), 46

J

- JavaScript vulnerability, 57

K

- KDC (Key Distribution Center), 8, 9
- Kerberos authentication, 7–9, 9
- keys. *See* cryptography; PKI

L

- L2TP (Layer 2 Tunneling Protocol), 44
- land attacks, 21
- LDAP (Lightweight Directory Access Protocol), 61, 61, 111
- logging. *See* auditing
- logic bombs, 30

M

- M of N (key) control, 140
- MAC (Mandatory Access Control), 4–5, 6, 164, 168, 169

190 **MAC (message authentication code) values – operational/organizational security****MAC (message authentication code)**

values, 119, 120

macro viruses, 29

maintenance hooks, 21

malicious code, *See also* attack;

Security+

defined, 29

exam essentials on, 30

logic bombs, 30

Trojan horses, 30

viruses, 29

worms, 30

man-in-the-middle attacks, 23, 23

mantraps, 152, 152

mathematical attacks, 25

MD (Message Digest) algorithms,

120, 121

media security, *See also* infrastructure

CDs/DVDs, 88

coaxial cable, 83, 83–85

exam essentials on, 88–89

fiber optic cable, 87, 87

flashcards, 88

floppies/diskettes, 88

hard drives, 88

overview, 82

removable media, 87–88

shielded cabling, 85–86, 85–86,

154, 154

smartcards, 88

tape drives, 87

unshielded cabling, 85–86, 85–86

MIME headers, corrupted, 51, *See also*

S/MIME

mitigation of risk, 172

mobile devices, 82

modems, 79, 79

monitoring. *See* auditing

multi-homed firewalls, 76, 90, 90

N

NAT (Network Address Translation),
93, 93–94

need to know, 5, 164

network hardening, 106–107

network-based IDSs, 96, 96

NNTP (Network News Transfer
Protocol) servers, 109

nonrepudiation, 50, 126, 128

NOS (network operating system)
hardening, 103–105

notification documents, 176

NTFS (New Technology File
System), 105

O

objects, 4–5, 8

OCSIP (Online Certificate Status
Protocol), 132

100BaseT cable, 86

1000BaseT cable, 86

operational/organizational security,
150–180, *See also* Security+

business continuity

backups, 161

defined, 159

elements in planning, 159–160

exam essentials, 162

high availability/fault tolerance,
160–161

utilities, 160

disaster recovery

alternate sites, 157–158

backups, 156–157

exam essentials, 158–159

offsite storage, 157

overview, 156

- plans, 158
- secure recovery, 157
- forensics
 - chain of custody, 170
 - collection of evidence, 171
 - defined, 170
 - evidence preservation, 170–171
 - exam essentials, 171
- overview, 150
- physical security
 - access control, 150–153, 152
 - barriers, 151–152, 152
 - EMI/RFI shielding, 154, 154
 - environment factors, 153–155
 - exam essentials, 155–156
 - facility location, 154
 - fire suppression, 154–155
 - mantraps, 152, 152
 - overview, 150
 - security guards, 152
 - social engineering attacks, 153
 - wireless cells, 153
- privilege management
 - auditing, 169
 - centralized management, 168
 - decentralized management, 168
 - exam essentials, 169–170
 - MAC/DAC/RBAC access
 - control, 169
 - overview, 167–168
 - principle of least privilege, 168
 - privilege, defined, 168
 - privilege escalation, 169
 - single sign-on, 168
 - user/group/role management, 168
- review question answers, 180
- review questions, 178–179
- risk identification
 - asset identification, 172
 - exam essentials, 173
 - minimizing risk impact, 172
 - overview, 171–172
 - risk assessment formulas, 172
 - threat identification, 172
 - vulnerability management, 172
- security documentation
 - asset inventories, 176
 - change documentation, 176
 - classification labeling, 4, 176
 - destruction of, 177
 - environment hardening, 103
 - exam essentials, 177
 - guidelines, 175
 - incident responses, 166
 - logs/audit trails, 32–33, 176
 - notification documents, 176
 - overview, 175
 - retention/storage of, 176
 - standards, 175
 - systems architecture, 175
- security policy
 - acceptable use, 163
 - account lockout, 164
 - code of ethics, 165–166
 - defined, 163
 - disposal/destruction, 165
 - due care, 164
 - employee termination, 165
 - exam essentials, 166–167
 - hiring, 165
 - human resources, 165–166
 - incident response, 166
 - need to know, 164
 - password management, 164
 - separation of duties, 164
 - service level agreements, 165
 - user privacy, 164
- security training
 - communication, 174
 - education, 174

192 Orange Book specifications – privilege management

- exam essentials, 174–175
- on-line resources, 174
- overview, 173
- user awareness, 174
- Orange Book specifications, 5
- OS (operating system) hardening, 103–105

P

- packet filter firewalls, 76
- packet sequencing, 24
- packet sniffing attacks, 56–57, 63, 78
- PAP (Password Authentication Protocol), 9
- passive detection and response, 98
- passwords
 - cracking attacks, 12, 26–27, 120–121
 - defined, 12, 12
 - history, 164
 - management policy, 164
 - one-time passwords, 13
 - strong passwords, 12, 26
 - weak passwords, 12
- PAT (Port Address Translation), 94
- patches, 105
- PBX (Private Branch Exchange) systems, 80, 80
- penetration testing, 33
- PGP (Pretty Good Privacy), 50–51, 51
- physical security, *See also* operational
 - access controls
 - barriers, 151–152, 152
 - biometrics, 14–15, 152
 - mantraps, 152, 152
 - overview, 150–151
 - security guards, 152
 - environment factors
 - EMI/RFI shielding, 154, 154
 - facility location, 154
 - fire suppression, 154–155
 - overview, 153
 - wireless cells, 153
- exam essentials, 155–156
- overview, 150
- social engineering attacks, 153
- piggybacking, 152
- ping flood/ping of death attacks, 21
- PKI (Public Key Infrastructure), *See also* cryptography
 - certificate authorities, 129–131, 130
 - certificate policies, 131
 - certificate practice statements, 131
 - certificate revocation, 131–132, 132
 - defined, 10–11, 11, 122, 129
 - exam essentials, 134–135
 - trust models, 132–134, 133
 - trusted third parties, 10, 129
 - X.509 certificates, 129, 130
- policy. *See* security policy
- polymorphic viruses, 29
- POP (Post Office Protocol), 48
- PPTP (Point-to-Point Tunneling Protocol), 44
- principle of least privilege, 5, 6, 168
- print server hardening, 110
- printed data, disposal of, 165
- privacy policy, 164
- Private Branch Exchange (PBX) systems, 80, 80
- private IP addresses, 93–94
- private keys. *See* cryptography; symmetric encryption
- privilege management, *See also* operational
 - auditing, 169
 - centralized management, 168
 - decentralized management, 168

exam essentials, 169–170
 MAC/DAC/RBAC access control, 169
 overview, 167–168
 principle of least privilege, 5, 6, 168
 privilege, defined, 168
 privilege escalation, 169
 single sign-on, 168
 user/group/role management, 168
 proxies, 76
 public keys. *See* asymmetric encryption;
 cryptography

R

radio frequency disturbance, 154
 RADIUS (Remote Access Dial-In User
 Service), 42–43, 43
 RAID (Redundant Array of Independent
 Disks), 160, 161
 RAs (registration authorities), 131
 RAS (Remote Access Server), 43, 43, 80
 RBAC (Role-Based Access Control), 6,
 7, 168, 169
 RBAC (Rule-Based Access Control), 6
 realms, 8
 recovering keys from escrow, 140
 recovery. *See* disaster recovery
 remote access security, *See also*
 communication
 in 802.11/11x wireless, 40–41, 40, 65
 exam essentials, 47–48
 in IPSec protocols, 44–46, 45–46
 in L2TP protocol, 44
 overview, 39–40, 39
 in PPTP protocol, 44
 using RADIUS, 42–43, 43
 using Secure Shell, 44
 using TACACS, 43, 43

in virtual private networks, 41–42, 41
 vulnerabilities, 46–47
 remote calling, 80
 removable media, 87–88
 replay attacks, 24, 24
 reverse hash matching, 26, 120
 revocation, certificate, 131–132,
 132, 139
 RFC 1918, 93–94
 risk identification, *See also* operational;
 vulnerabilities
 asset identification, 172
 exam essentials, 173
 minimizing risk impact, 172
 overview, 171–172
 risk assessment formulas, 172
 threat identification, 172
 vulnerability management, 172
 routers, 76, 77–78, 77–78

S

S-HTTP (Secure-HTTP), 56
 S/FTP (Secure FTP), 62
 S/MIME (Secure Multipurpose Internet
 Mail Extensions), 49–50, 50
 secret (private) keys. *See* cryptography;
 symmetric encryption
 Security+ exam objectives, *See also* com-
 munication; cryptography;
 infrastructure; operational
 access control models
 defined, 3
 Discretionary Access Control, 5–6
 exam essentials on, 6–7
 Mandatory Access Control, 4–5
 overview, 3–4, 168, 169
 Role-Based Access Control, 6

- attack methods, *See also* attack
 - back door, 21–22, 22
 - birthday, 26, 120
 - buffer overflow, 27, 57–58
 - Denial of Service, 18–21, 19–20
 - exam essentials on, 28–29
 - man-in-the-middle, 23, 23
 - mathematical, 25
 - overview, 18
 - password cracking, 12, 26–27, 120–121
 - replay, 24, 24
 - social engineering, 31–32, 52–53
 - software exploitation, 27
 - spoofing, 22–23, 52
 - TCP/IP hijacking, 24, 25
 - weak keys and, 25
- auditing, 32–33
- authentication methods, *See also* authentication; certificates
 - biometrics, 14–15, 152
 - certificates, 10–11, 11
 - CHAP, 9–10, 10
 - defined, 7
 - exam essentials on, 15
 - Kerberos, 7–9, 9
 - multi-factor authentication, 13–14, 14
 - mutual authentication, 14
 - tokens, 13, 13
 - usernames/passwords, 12, 12
- malicious code
 - defined, 29
 - exam essentials on, 30
 - logic bombs, 30
 - Trojan horses, 30
 - viruses, 29
 - worms, 30
- non-essential services, 15–17
- review question answers, 36
- review questions, 34–35
- security associations, 46
- security baselines, 103
- security devices, *See also* infrastructure
 - exam essentials on, 82
 - firewalls, 74–77, 75, 77, 95, 96
 - Intrusion Detection Systems, 81, 95–102, 96–101
 - mobile devices, 82
 - modems, 79, 79
 - for monitoring/diagnostics, 81
 - Remote Access Server, 80
 - routers, 77–78, 77–78
 - servers, 81
 - switches, 78, 78
 - Telecom/PBX systems, 80, 80
 - virtual private networks and, 81
 - wireless networks, 79
 - workstations, 81
- security documentation, *See also* operational
 - asset inventories, 176
 - change documentation, 176
 - classification labeling, 4, 176
 - destruction of, 177
 - environment hardening, 103
 - exam essentials, 177
 - guidelines, 175
 - incident responses, 166
 - logs or audit trails, 176
 - notification documents, 176
 - overview, 175
 - retention/storage of, 176
 - standards, 175
 - systems architecture, 175
- security domains, 4–5
- security guards, 152
- security policy, *See also* operational
 - acceptable use, 163
 - account lockout, 164

- certificates, 131
- code of ethics, 165–166
- defined, 163
- disposal/destruction, 165
- due care, 164
- employee termination, 165
- exam essentials, 166–167
- firewalls, 76
- hiring, 165
- human resources, 165–166
- incident response, 166
- need to know, 164
- password management, 164
- separation of duties, 164
- service level agreements, 165
- user privacy, 164
- security topologies, *See also*
 - infrastructure
 - defined, 89
 - demilitarized zones, 90, 90
 - exam essentials on, 94–95
 - extranets, 90, 91
 - intranets, 90, 91
 - IP address translation and, 93–94, 93
 - RFC 1918 and, 93–94
 - security zones, 89–90, 89–91
 - tunneling and, 94
 - virtual LANs, 91–92, 92
- security training, *See also* operational
 - communication, 174
 - education, 174
 - exam essentials, 174–175
 - on-line resources, 174
 - overview, 173
 - user awareness, 174
- sensitivity labels, 4–5
- separation of duties policy, 164
- server clustering, 160, 162
- server rooms, mission-critical, 151, 151, 154
- servers, 81
- service level agreements (SLAs), 165
- service packs, 105
- services, non-essential, 15–17
- shielding, 85–86, 85–86, 154, 154
- signature detection in IDSs, 97, 98
- signatures, digital. *See* digital
- single points of failure, 160
- single sign-on, 8, 168
- site surveys, 66
- SLE (Single Loss Expectancy)
 - formula, 172
- smartcards, 13, 13–14, 88
- SMTP relay, 58–59
- SMTP (Simple Mail Transport Protocol), 48, 49
- smurf attacks, 19, 20
- sniffing attacks, packet, 56–57, 63, 78
- SNMP (Simple Network Management Protocol), 81
- social engineering attacks, 31–32, 52–53, 153
- software exploitation attacks, 27
- spam, 52
- spoofing attacks, 22–23, 52
- SSH (Secure Shell), 44
- SSL (Secure Sockets Layer), 55–56
- standards, 175
- stateful inspection firewalls, 76
- storage
 - encryption keys, 138–139, 139, 140
 - media, disposal of, 165
 - media, storing offsite, 157
 - security documentation, 176
- STP (shielded twisted pair) cable, 85–86, 85–86, 154
- stream cipher cryptography, 122
- strong authentication, 14

strong passwords, 12, 26
 STs (Service Tickets), 8, 9
 subjects, 4–5, 8
 switches, 78, 78
 symmetric encryption, 46, 121–122,
 126–127, 127
 SYN flood attacks, 20, 20
 system hardening, 16
 system scanning, 33
 systems architecture documentation, 175

T

T-connectors, 84
 TACACS (Terminal Access Controller
 Access Control System), 43, 43
 tape drives, 87
 TCP SYN flood attacks, 20, 20
 TCP/IP hijacking attacks, 24, 25
 TCSEC (Trusted Computer System Eval-
 uation Criteria), 5
 teardrop attacks, 20
 Telecom/PBX systems, 80, 80
 Telnet, 44
 10Base2/Thinnet cable, 83
 10Base5/Thicknet cable, 83
 10BaseT cable, 85, 86
 terminals, 81
 termination, coax cable, 83, 85
 TGTs (Ticket Granting Tickets), 8, 9
 threats, 172, *See also* attack; risk;
 vulnerabilities
 timestamps, packet, 24
 TLS (Transport Layer Security), 55, 56
 tokens, 13, 13
 training. *See* security training
 transport mode in IPSec, 45, 46
 Trojan horses, 30

trust models, 132–134, 133
 trusted third parties, 10, 129
 tunneling protocols, 42, 94, *See also*
 IPSec; L2TP; PPTP

U

updating
 applications, 107
 networks, 106
 OSs/NOSs, 105
 user awareness of security, 174
 user privacy policy, 164
 username/password authentication,
 12, 12
 utilities, physical, 160
 UTP (unshielded twisted pair) cable,
 85–86, 85–86

V

valid from/valid to dates, 139
 vampire taps, 83, 84
 viruses, 29
 VLANs (virtual local area networks), 78,
 91–92, 92
 VPN protocols, 42, 94, *See also* IPSec;
 L2TP; PPTP
 VPNs (virtual private networks), 41,
 41–42, 81
 vulnerabilities, *See also* attack; risk;
 threats
 in cryptography
 hashing, 26, 120–121
 key recovery, 140
 key storage, 137, 138
 weak keys, 25
 defined, 172

- in e-mail security
 - hoaxes, 52–53
 - MIME headers, 51
 - open relays, 59
 - overview, 51
 - SMTP relays, 58–59
 - spam, 52
 - spoofed e-mail, 52
 - in File Transfer Protocol, 63
 - in Internet security
 - ActiveX, 57
 - buffer overflows, 57–58
 - Common Gateway Interface, 58
 - cookies, 58
 - HTTP protocol, 54–55, 55, 56
 - instant messaging, 56–57
 - JavaScript, 57
 - signed applets, 58
 - SMTP relay, 58–59
 - in physical security
 - EMI disturbance, 85, 86, 154, 154
 - fire, 154
 - radio frequency disturbance, 154
 - social engineering, 153
 - wireless cells, 153
 - privilege escalation, 169
 - in remote access, 46–47
 - in wireless networks, 66
 - vulnerability scanning, 33
-
- W**
- WAP (Wireless Application Protocol), 64–65, 65
-
- war dialing attacks, 79
- warm sites, 157
- weak keys, 25
- web server hardening, 108
- wireless security, *See also* communication
 - in 802.11/11x networks, 40–41, 40, 65
 - exam essentials on, 66–67
 - overview, 64, 79
 - site surveys, 66
 - vulnerabilities, 66
 - using Wired Equivalent Privacy, 65
 - wireless cells, 153
 - using WTLS in WAP protocol, 64–65, 65
- workstations, 81
- worms, 30
- WTLS (Wireless Transport Layer Security), 64
-
- X**
- x.500 standard, 61
- X.509 certificates, 129, 130
-
- Z**
- Zimmerman, Phillip R., 50
- zombies, 18–19, 19
- zone transfers, 109